



CHECKLIST RGDP

**GARANTA A
CONFORMIDADE**

BOAS PRÁTICAS GERAIS

- ☐ Reavaliar e reformular as políticas de privacidade, todos os textos e impressos que prestem informação aos titulares, garantindo que as informações transmitidas aos utilizadores devem ser feitas de forma concisa, inteligível e com uma linguagem clara e simples.
- ☐ Garantir o consentimento do cidadão para o tratamento de dados pessoais.
- ☐ Documentar as melhores práticas de proteção de dados e divulgar a toda a Organização.
- ☐ Implementar um processo de resposta em caso de incidente de violação de dados pessoais.
- ☐ Aderir a um código de conduta ou a um procedimento de certificação operado por um dos organismos de certificação acreditados por uma Autoridade de Proteção de Dados.
- ☐ Criar um processo de verificação de idade e obtenção de consentimento parental no caso de menores.
- ☐ Mapear e categorizar os dados pessoais recolhidos e tratados, bem como onde estão alojados e quem pode aceder.
- ☐ Avaliar a natureza dos tratamentos de dados efetuados, caso se tratem de dados sensíveis, aplicar as condições específicas definidas pelo Regulamento para o seu tratamento, como a contratação de um Encarregado de Proteção de Dados.
- ☐ Implementar tecnologias e mecanismos de segurança, que garantam a proteção dos dados.
- ☐ Encriptar todos os ficheiros e sistemas que tenham dados pessoais.

02

TOUCH POINTS

- ☐ Rever todos os touch points de geração de leads ou obtenção de dados pessoais e garantir a conformidade com todas as medidas do RGPD.
- ☐ Criar uma lista com cada touch point (website; Landing Page; forms; mailings, parceiros de media; folhetos; brochuras, etc.) e com links diretos para cada um ou com uma imagem do ficheiro, indicando a data de revisão e o responsável pela revisão.

03

PARCEIROS DE COMUNICAÇÃO

- ☐ Rever contratos com entidades terceiras e responsáveis de tratamento de dados em regime de subcontratação e garantir que estão em conformidade com as medidas do RGPD.
- ☐ Solicitar a todos os parceiros a confirmação por escrito de que estão em conformidade com o RGPD, nomeadamente as regras de consentimento e as regras sobre transferência de dados além-fronteiras.
- ☐ Criar uma lista com o nome do parceiro, a informação de contacto, se cumpre as regras de obtenção de consentimento ou não, se cumpre a regra de transferência de dados ou não, a data em que ficaram em conformidade com o RGPD e o link para documento assinado ou imagem do ficheiro.

[DOWNLOAD - TEMPLATE DE PARCEIROS DE COMUNICAÇÃO](#)

SITE

- ☐ Implementar certificado de segurança HTTPS.
- ☐ Implementar restrições aos mecanismos de digital body language (ex.: heatmap ou mouseflow) sempre que essa informação possa ser associada a um determinado indivíduo que não deu consentimento para esse efeito.
- ☐ Implementar aviso e discriminação da política de Cookies.
- ☐ Facilitar o acesso à consulta da política de privacidade.

PRIVACIDADE DE DADOS DADOS PESSOAIS

- ☐ Criar página online que permita:
- ☐ Expor todas as informações sobre as políticas de privacidade, indicando:
 - Finalidade do tratamento;
 - Direito a apresentar reclamação a uma autoridade;
 - Existência de decisões automatizadas;
 - Categoria dos dados;
 - Prazo de conservação;
 - Eventuais destinatários;
 - Identidade e contactos do responsável pelo tratamento;
 - Contacto do encarregado da proteção de dados (se aplicável);
 - Se o tratamento for necessário para prosseguir interesses legítimos, referi-los;
- ☐ Obter o consentimento granular, isto é, com um opt-in por cada atividade de marketing e autorização para partilha de dados com entidades terceiras, caso se verifique.
- ☐ Dar ao titular de dados a possibilidade de exercer os seus direitos, nomeadamente, consultar, retificar, pedir a portabilidade, oposição ao profiling ou eliminação dos dados.

FORMULÁRIOS

- ☐ Garantir que não há caixas de consentimento previamente preenchidas.
- ☐ Colocar check-box para aceitação dos termos de consentimento e privacidade de dados em todos os formulários.
- ☐ Usar double opt-in nos formulários de angariação de dados.

MAILINGS

- ☐ Todos os e-mails devem ter no rodapé os dados do remetente, os destinatários, opção de saída da mailing list, e consulta de condições de privacidade.
- ☐ Enviar email marketing apenas para indivíduos que tenham dado consentimento para esse propósito.

CRM

- ☐ Criar automatismos que simplifiquem a conformidade com o Regulamento.
- ☐ Criar campo no CRM para registo de consentimento e da como foram obtidos os dados.
- ☐ Garantir que atividades diferentes de marketing têm opções de consentimento separadas (p.e.: subscrição newsletter; aceitação de ações de telemarketing; aceitação de mecanismos de monitorização online) e que são implementadas regras de negócio que respeitem as opções dos titulares dos dados.
- ☐ Garantir que o sistema permite a auditoria a todas as atividades, alterações e pessoas que interagiram cada um dos dados pessoais ao nível da entidade.



Instituto Pedro Nunes - Incubadora
Rua Pedro Nunes, Edifício C
3030-199 Coimbra - PORTUGAL

+351 239 700 300
hello@liminal.pt
www.liminal.pt