A sua empresa não nomeou DPO.

Tem a certeza de que consegue
justificar essa decisão?

RGPD - Artigo 37.º | WP29 / EDPB

QUANDO O DPO É OBRIGATÓRIO

O artigo 37.º não deixa tudo em aberto.

A designação é obrigatoria em três cenarios principais.

1

Autoridade ou organismo público

Com a ressalva das jurisdições no exercicio da sua função judicial.

2

Monitorização regular e sistemática em grande escala

Quando as atividades principais implicam acompanhamento recorrente, estruturado e relevante de titulares de dados.

3

Tratamento em grande escala de dados sensíveis ou dados penais

Inclui categorias especiais de dados e dados relativos a condenações penais e infrações, quando o tratamento faz parte do núcleo do negócio.

Não basta perguntar se a empresa é grande. É preciso perceber o que trata, como trata e porque trata.

O ERRO MAIS COMUM

“Somos PME, logo não precisamos de precisamos de DPO.”

Esse raciocínio é insuficiente, e muitas vezes juridicamente fraco.

O que realmente pesa:

- as atividades principais da organização
- a existência de monitorização regular e sistematica
- a escala do tratamento
- a natureza sensível dos dados tratados

Tamanho, por si só, não decide a a questao.

Uma empresa pequena pode ter obrigacão de designar DPO. E uma empresa maior pode não a a ter. O ponto critico é a configuracao real do tratamento.

Se a analise interna comeca e termina no número de trabalhadores, a decisão nasce torta.

ACCOUNTABILITY

Não nomear DPO pode ser legítimo. legítimo.

O que não pode faltar e uma posição interna defensável e demonstrável.

1. O RGPD não diz literalmente “documente a não designação”.
Mas exige que a organização consiga demonstrar que avaliou corretamente a sua posição.

2. O WP29 / EDPB recomendam documentar a análise.

Sobretudo quando a resposta não é óbvia, a decisão deve ficar registada internamente.

3. Sem registo, a conclusão fica frágil.

Em auditoria, incidente ou pedido de esclarecimento, a organização terá de mostrar o raciocinio que seguiu, não apenas a resposta final.

Decidir sem rasto interno é transformar uma opção jurídica numa vulnerabilidade de vulnerabilidade de governance.

CHECKLIST INTERNA

Se não nomear DPO, o que deve ficar ficar documentado?

Não precisas de um memo ornamental. Precisas de uma análise clara.

- descrição das atividades principais
- avaliação de monitorização regular e sistematica
- análise da escala do tratamento
- tipologia e sensibilidade dos dados
- conclusão fundamentada e data da decisão
- momento previsto para reavaliação

Quanto mais cinzenta for a situação, mais importante é o registo da análise.

SINAIS DE ALERTA

A decisão de não designar DPO pode pode estar errada se...

...o negócio real da organização disser uma coisa e a narrativa interna disser outra.

Videovigilância, scoring, profiling ou geolocalização

Se o negócio assenta em observação recorrente de titulares, há um risco sério de enquadramento.

Dados de saúde, biometria ou outros dados sensíveis em volume relevante

A escala e a natureza do tratamento podem empurrar a organização para a obrigatoriedade.

Decisão antiga nunca revista

Uma conclusão de há tres anos pode ja não refletir a operação atual, os sistemas ou os fluxos de dados.

Analise reduzida a “não somos grandes”

Se este foi o criterio central, provavelmente a avaliação ficou aquém do que era exigivel.

Quando há dúvida séria, o pior caminho é a autoconfiança sem análise.

O teste que interessa não e “temos DPO?”

Mas sim:

Conseguimos defender a decisão que que tomamos?

Na **Ahkoris**, ajudamos a avaliar se existe obrigação de designar DPO e a documentar uma posição técnicamente defensável.

Se a decisão nunca foi testada com rigor, este e o momento certo para a rever.