KINGFISHER PLC

Norma de proteção de dados

Proprietário do documento:	Responsável pela proteção de dados do Grupo
Documento à atenção de:	Todas as empresas Kingfisher
Política subjacente	Política de proteção de dados
Data da próxima revisão:	9 de janeiro de 2019
Documento(s) de política(s) relacionada(s):	Política de proteção de dados, Política de retenção de documentos e conservação de registos, Política de segurança das informações das normas de retenção de documentos e de conservação de registos, Política de utilização aceitável

Conteúdo

1. Resumo e objetivo(s)

O propósito da presente Norma de política consiste em garantir a conformidade com as leis de proteção de dados e privacidade e em garantir que os dados dos nossos clientes, funcionários e fornecedores são sempre recolhidos e utilizados adequadamente, em qualquer jurisdição em que as empresas do Grupo Kingfisher atuem.

Na presente Norma de política, "**Dados Pessoais**" são informações que, isoladamente ou em combinação com outras informações, permitem a identificação de uma pessoa ("**Indivíduo**"). Isto inclui, por exemplo: o endereço de e-mail profissional de um indivíduo, o seu nome próprio em conjunto com o endereço postal ou a data de nascimento, uma fotografia de um Indivíduo, etc…

Os Dados Pessoais têm de ser sempre mantidos em segurança e tratados de forma equitativa, transparente e em conformidade com a lei.

Cada empresa do Grupo tem de conhecer o quadro regulamentar aplicável aos territórios em que atua.

- Na União Europeia, o Regulamento Geral de Proteção de Dados da UE (RGPD) [Regulamento (UE) 2016/679] é aplicável a partir de 25 de maio de 2018, em conjunto com outras leis relacionadas com a privacidade ou regras locais de proteção de dados;
- Fora da União Europeia, têm de ser cumpridas quaisquer leis locais ou regionais aplicáveis às atividades das empresas do Grupo.

O responsável pela proteção de dados do Grupo com o apoio da pessoa que, em cada país onde a Kingfisher atua, é responsável pelas questões de proteção de dados ("**delegado de proteção de dados do país**") irá estabelecer e impor procedimentos eficazes de conformidade.

2. Responsabilização e governança

2.1 O RESPONSÁVEL PELA PROTEÇÃO DE DADOS do Grupo é responsável pela presente Norma política e pela sua aplicação em todo o Grupo.

O papel e as responsabilidades do responsável pela proteção de dados são as seguintes:

- manter o Conselho de Administração atualizado em matéria de responsabilidades, riscos e questões associados à proteção de dados;
- rever e aprovar regularmente todos os procedimentos e políticas de proteção de dados;
- monitorizar a conformidade com os procedimentos, políticas e leis aplicáveis de proteção de dados e privacidade;
- organizar formação e aconselhamento em matéria de proteção de dados para todos os membros do pessoal e todos os abrangidos pela presente política;

- responder a perguntas do pessoal, membros do Conselho de Administração e outras partes interessadas acerca de proteção de dados;
- responder a indivíduos, tais como clientes e funcionários, que desejem saber quais os dados mantidos a seu respeito, bem como verificar e aprovar quaisquer contratos ou acordos relativos a processamento de dados celebrados com terceiros que tratem os dados da empresa;
- supervisionar e rever avaliações de impacto na privacidade;
- ser um ponto de contacto para a principal autoridade supervisora e colaborar com as autoridades locais.

O responsável pela proteção de dados pode ser contactado através de dpo@kingfisher.com

Tenha em atenção que todas as empresas Kingfisher e todos os cargos dentro do Grupo estão obrigados a divulgar, sem demora indevida, quaisquer informações de que o responsável pela proteção de dados possa precisar, dentro do razoável, para cumprir o seu papel.

2.2 O DELEGADO DE PROTEÇÃO DE DADOS DO PAÍS é responsável por:

- ajudar o responsável pela proteção de dados a compreender a legislação local a respeito da privacidade e as leis de proteção de dados;
- ajudar o responsável pela proteção de dados a definir regras e processos de proteção de dados em determinado país ou território onde as empresas do Grupo Kingfisher atuem;
- fazer a ligação, relativamente a questões de proteção de dados e privacidade, entre o responsável pela proteção de dados e as empresas do Grupo Kingfisher em causa em determinado país.

Está disponível na Intranet uma lista de delegados de proteção de dados de país e o Departamento de Comunicações internas irá comunicar regularmente as atualizações.

2.3 A EQUIPA DE GOVERNANÇA DE TI é responsável por garantir a segurança dos dados nos sistemas da Kingfisher e de terceiros.

A equipa de governança de TI deve ser sempre consultada caso os dados sejam processados por uma empresa do Grupo ou por terceiros. Os pontos de contacto dentro da equipa de governança de TI encontram-se detalhados na Intranet, e o Departamento de Comunicações Internas irá comunicar regularmente as atualizações.

Papel e responsabilidades da equipa de governança de TI:

- garantir que todos os sistemas, serviços, software e equipamentos cumprem os padrões de segurança aceitáveis;
- garantir que todos os sistemas, serviços, software e equipamentos permitem a conformidade com as políticas, processos, diretrizes e leis de proteção de dados dos países em causa;

- elaborar políticas de segurança e documentos contratuais para sistemas e informações;
- realizar as devidas diligências no que respeita a terceiros.

3. Padrões mínimos do Grupo

A menos que as leis de uma jurisdição onde as empresas do Grupo Kingfisher atuem imponham requisitos mais exigentes (caso em que se aplicarão os referidos requisitos mais exigentes), os seguintes padrões deverão ser sempre cumpridos em todo o Grupo Kingfisher aquando do tratamento de Dados Pessoais de funcionários, clientes e fornecedores. Regras mais detalhadas e específicas de cada país serão comunicadas a cada empresa do Grupo Kingfisher pelo responsável pela proteção de dados ou pelo delegado de proteção de dados do país.

3.1 Recolha de dados:

Antes da recolha de Dados Pessoais:

- temos de nos assegurar de que recolhemos apenas o mínimo de dados pessoais necessário para a finalidade em causa;
- temos de nos assegurar de que a finalidade da recolha é legítima e não viola os direitos dos indivíduos;
- temos de informar os indivíduos, de forma clara, da utilização que pretendemos dar aos seus Dados Pessoais, bem como dos motivos para a recolha;
- temos de nos assegurar de que os Dados Pessoais serão recolhidos e armazenados de forma segura e de que estão instituídas medidas de segurança adequadas para evitar o acesso não autorizado, perdas ou danos aos Dados Pessoais.

3.2 Tratamento dos dados:

- temos de nos assegurar de que os Dados Pessoais não estão disponíveis para pessoas que não precisam de ter acesso a eles;
- temos de nos assegurar de que os Dados Pessoais são utilizados apenas para os fins para os quais foram recolhidos e dentro do razoavelmente expectável por parte do indivíduo a que referem;
- temos de verificar e confirmar regularmente que os dados são tratados e armazenados de forma segura e protegidos contra acesso não autorizado, perdas ou danos;
- temos de identificar e de registar sempre num formato a comunicar pelo responsável pela proteção de dados as seguintes informações: (i) categorias dos dados recolhidos e tratados, (ii) categorias de indivíduos cujos dados serão processados, (iii) categorias dos destinatários a quem os Dados Pessoais foram ou serão divulgados, (iv) endereço(s) do(s) local(ais) onde os dados são armazenados.
- O responsável pela proteção de dados ou o delegado de proteção de dados devem ser sempre contactados antes da utilização de qualquer ferramenta de processamento automatizado que vá resultar em tomadas de decisão acerca de um indivíduo, ou seja, da avaliação de determinados aspetos pessoais do indivíduo para analisar ou prever certos aspetos sobre o seu desempenho no

trabalho, situações económicas, estado de saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou movimento

3.3 Transferência de dados:

Antes de concordar em conceder o acesso (por transferência ou acesso remoto) a Dados Pessoais a qualquer entidade de processamento exterior ao Grupo Kingfisher:

- temos de nos assegurar de que a entidade de processamento para a qual transferimos Dados Pessoais cumpre a presente Norma e a legislação aplicável;
- temos de identificar e de registar sempre as seguintes informações: (i) nome e dados de contacto do representante da entidade de processamento e do responsável pela proteção de dados, (ii) categorias dos dados tratados, (iv) categorias dos indivíduos cujos dados serão processados, (v) endereço(s) do(s) local(ais) para onde os dados serão transferidos e/ou a partir dos quais serão0 acedidos, (vi) lista e informações empresariais de quaisquer entidades de processamento secundárias e (vi) categorias dos destinatários a quem os Dados Pessoais foram ou serão divulgados;
- temos de nos assegurar de que nenhuns Dados Pessoais são transferidos para/acedidos a partir de outro país ou território, a menos que o país ou território em causa assegure um nível adequado de proteção dos direitos e liberdades dos indivíduos no que diz respeito ao processamento de dados pessoais, ou que é assinado, entre as partes, um contrato escrito que contenha garantias suficientes (ou que existem providências alternativas para fornecer tais garantias, em conformidade com as leis aplicáveis de proteção de dados).

3.4 Retenção de dados

Os Dados Pessoais não devem ser conservados por tempo superior ao necessário para os fins para que foram recolhidos (secção 3.1 acima). Isto significa que os dados devem ser destruídos ou eliminados de forma segura dos sistemas da empresa quando deixam de ser necessários.

Exemplo: Um cliente entrou num concurso para ganhar uma nova ferramenta elétrica, preenchendo um formulário com o seu nome, morada e número de telefone, e assinalou uma caixa para declarar que não deseja receber qualquer comunicação adicional da empresa do Grupo. Após a realização do sorteio, a empresa do Grupo deve eliminar os dados do cliente apresentados no formulário, uma vez que já não são necessários para os fins para que foram obtidos.

A política da Kingfisher acerca de retenção de documentos e a legislação acerca do tempo de retenção têm de ser cumpridas.

3.5 Direitos dos indivíduos

Os dados têm de ser processados em conformidade com os direitos dos indivíduos. Os direitos dos indivíduos variam de país para país. Na União Europeia, os indivíduos, em geral, têm o direito de:

(a) retirar o consentimento que deram para que os seus Dados Pessoais fossem processados (se o processamento for realizado com base nesse consentimento);
(b) se oporem ao processamento dos seus Dados Pessoais (mesmo que o processamento seja realizado com base em interesses legítimos);
(c) obter acesso a quaisquer Dados Pessoais acerca de si próprios;
(d) solicitar a correção de quaisquer Dados Pessoais incorretos;
(e) solicitar a eliminação dos seus Dados Pessoais dos sistemas da empresa;
(f) solicitar a transferência dos seus dados pessoais para outras empresas;
(g) evitar processamento suscetível de causar perdas ou sofrimento aos próprios ou a outrem.

3.6 Reclamações e infrações

Todas as reclamações e infrações, incluindo qualquer falha de segurança, que afetem Dados Pessoais têm de ser imediatamente comunicadas ao responsável pela proteção de dados e/ou a quaisquer delegados.

Quaisquer reclamações por falha de segurança que afetem Dados Pessoais têm de ser imediatamente comunicadas ao chefe de governança de TI.

Qualquer roubo, utilização indevida ou falha de segurança que conduza à destruição, perda, alteração ou divulgação/acesso não autorizados a Dados Pessoais tem de ser imediatamente (e, em quaisquer circunstâncias, no prazo máximo de 2 horas) comunicado ao responsável pela proteção de dados e ao chefe de governança de TI.

4. Monitorização e auditoria

Periodicamente, será realizada uma auditoria de conformidade com a presente Norma de política e outros processos relacionados com a proteção de dados e as regras emitidas pelo responsável pela proteção de dados ou os delegados de proteção de dados de país.

Em caso de qualquer dúvida quanto à matéria da presente Norma de política, deve aconselhar-se junto do responsável pela proteção de dados do Grupo ou do delegado de proteção de dados para o seu país.

Pode também utilizar a linha direta de denúncia para relatar as suas preocupações.

5. Visão geral dos consentimentos e aprovações

Ação/situação	Comunicação		A quem/por parte de quem?
	Notificação (prévia)	Aprovação prévia	
Falha de segurança	X		Responsável pela proteção de dados do Grupo* + chefe de governança
Tomada de decisão automatizada (incluindo análise de perfis)	X	X	Responsável pela proteção de dados do Grupo* + chefe de governança
Reclamações de indivíduos a quem os dados dizem respeito	X		Responsável pela proteção de dados do Grupo
Inquéritos regulamentares	X		Responsável pela proteção de dados do Grupo + diretor jurídico do Grupo
Medida coerciva regulamentar	X		Responsável pela proteção de dados do Grupo + diretor jurídico do Grupo
Exercício dos direitos dos indivíduos a quem os dados dizem respeito	X		Responsável pela proteção de dados do Grupo
Novas atividades de processamento que exigem uma avaliação do impacto na privacidade dos dados	X	X	Responsável pela proteção de dados do Grupo* + chefe de governança

*Em todos os casos, quer diretamente, quer através do delegado de proteção de dados do país.