Política Global de Privacidade e Proteção de dados

Introdução

A Crawford & Company e suas subsidiárias majoritárias e controladas (coletivamente "Crawford" ou "Empresa") adotaram a Política Global de Privacidade e Proteção de dados ("Política"). A Crawford reconhece a importância da privacidade e da segurança, e tem o compromisso de cumprir as leis aplicáveis de proteção de dados e os requisitos contratuais do cliente na administração de dados pessoais.

Objetivo

Embora as leis de proteção de dados variem por jurisdição, todo o pessoal da Crawford deve estar ciente de que as leis existem para proteger a privacidade e a segurança dos dados pessoais, e estas leis impactam a maneira como a Crawford e seu pessoal usam, divulgam ou processam tais informações.

Esta Política Global de Privacidade e Proteção de dados ("Política"):

- estabelece os princípios que se aplicam ao processamento de dados pessoais pela Crawford, e descreve como a Crawford cumpre esses princípios; e
- oferece uma visão geral da estrutura de governança de privacidade da Crawford, e as funções e responsabilidades dos principais grupos e pessoas no cumprimento das obrigações e tarefas de conformidade da Crawford.

Esta Política será complementada por políticas, procedimentos e diretrizes adicionais para abordar áreas, jurisdições, leis e requisitos específicos.

Escopo

Esta Política se aplica a todos os dados pessoais processados pela Crawford como controladora ou processadora de dados, inclusive os dados relativos ao seu pessoal, clientes, demandantes, prestadores de serviço e outras partes. Todo o pessoal deve cumprir esta Política. O funcionário que violar esta Política pode estar sujeito a medidas disciplinares segundo a legislação local ou termos laborais aplicáveis.

Todos os funcionários têm um papel importante a desempenhar na gestão adequada e na salvaguarda de dados pessoais, para identificar problemas de manuseio e proteção de dados à medida que surgem, e para encaminhá-los imediatamente ao Escritório de Privacidade Global (Global Privacy Office). Todos os funcionários também devem cooperar conforme necessário para a implementação de princípios, requisitos e componentes-chave desta Política.

Princípios

1. **Processamento justo, transparente e legal**. Dados pessoais serão

coletados, armazenados e processados de maneira justa, legal e transparente. Isso significa que:

1.1. As pessoas serão informadas do processamento (pelo controlador de dados).

1.2. Os dados pessoais são processados segundo a finalidade declarada para sua coleta ou para propósitos compatíveis semelhantes, e estão sujeitos a uma base legal, tal como consentimento, onde exigido por lei.

1.3. Os dados pessoais não são processados de formas não esperadas razoavelmente pelo titular dos dados.

1.4. Ao agir como processador de dados, os dados pessoais só serão processados conforme necessário para executar os serviços conforme orientado pelos clientes, ou onde, de outra forma, for exigido pela legislação aplicável.

2. **Minimização de dados.** Os dados pessoais serão coletados apenas onde razoável e necessário para os fins declarados para os quais estão sendo processados, e serão adequados, relevantes e limitados ao que é necessário em relação a esses propósitos.

3. **Limite de propósito.** Os dados pessoais serão processados para fins específicos, explícitos e legítimos, e de uma maneira compatível com o propósito para o qual foram inicialmente coletados.

4. **Precisão.** Os dados pessoais serão precisos e atualizados.

4.1. Serão tomadas medidas razoáveis para assegurar a precisão dos dados pessoais obtidos.

4.2. Dados pessoais imprecisos (considerando o propósito de seu processamento) serão eliminados ou retificados.

5. **Retenção limitada.** Os dados pessoais serão retidos apenas enquanto forem necessários para atingir o(s) fim(ns) específico(s) e estarão sujeitos às leis de proteção de dados aplicáveis e aos requisitos contratuais dos clientes.

6. **Segurança e integridade.** Medidas apropriadas de segurança organizacional, administrativa e técnica serão implementadas para salvaguardar os dados pessoais, oferecer processamento seguro para eles, além de identificar, prevenir, detectar e mitigar riscos aos dados pessoais, sistemas, ferramentas e processos usados para processar dados pessoais.

6.1. Os dados pessoais serão processados de uma maneira que ofereça segurança apropriada deles.

6.2. Medidas de segurança precisam ser concebidas e implementadas para proteger contra processamento ilegal e não autorizado, e perda, destruição ou dano acidental dos dados pessoais e sistemas correlatos.

6.3. Serão concebidos e implementados controles para detectar, mitigar e corrigir eventos e incidentes de segurança.

6.4. Serão estabelecidas políticas e procedimentos para que tais eventos e incidentes de segurança e privacidade sejam imediatamente relatados internamente, e investigados, avaliados e administrados segundo as leis de proteção de dados estabelecidas, onde possam impactar os dados pessoais ou atividades de processamento correlatas.

7. **Concepção de privacidade.** Atividades e processos serão concebidos, implementados e realizados de forma que ofereçam, desde o princípio, conformidade com os princípios supracitados e a integração de salvaguardas necessárias para dados pessoais.

8. **Responsabilidade.**

A conformidade com estes princípios será avaliada e as atividades de processamento serão conduzidas de forma que demonstrem conformidade e possam ser auditadas e avaliadas.

8.1. Consultas e reclamações relacionadas ao processamento de dados pessoais serão avaliadas, respondidas e resolvidas (dentro do possível) de maneira justa e sem atraso injustificado.

8.2. Processos razoáveis para receber, administrar e responder a perguntas, solicitações e reclamações de pessoas e clientes são estabelecidos para fornecer respostas justas, oportunas, coerentes e em conformidade com a lei.

8.3. Registros precisos de atividades de processamento serão mantidas, incluindo registros de incidentes de segurança, reclamações, solicitações do titular dos dados e outros registros obrigatórios segundo as leis aplicáveis de proteção de dados.

Principais componentes de conformidade com a privacidade

A fim de cumprir todos os princípios supracitados, a Crawford precisa tomar medidas para assegurar que estes princípios sejam abordados dentro de todos os processos e atividades comerciais relevantes, e implementar determinados processos e procedimentos, que incluam os seguintes componentes principais, cada um dos quais é abordado abaixo nesta Política:

- Notificação às pessoas físicas

- Base legal de processamento
- Manutenção de registros (e registros de processamento)
- Direitos do titular dos dados
- Gestão de terceiros e prestadores de serviço
- Resposta a incidentes
- Conscientização e treinamento referentes à privacidade
- Avaliações de impacto à privacidade
- Avaliações e auditorias contínuas
- Governança

Notificação às pessoas físicas

A Crawford notificará os titulares dos dados pessoais que ela os processa segundo exigido pela lei de proteção de dados, incluindo aviso do seguinte: os tipos de dados pessoais coletados, os propósitos do processamento, método de processamento, os direitos do titular dos dados com relação a seus dados pessoais, o período de retenção, possíveis transferências internacionais de dados, se eles serão compartilhados com terceiros e as medidas de segurança da Empresa para protegê-los.

Para os funcionários, estas informações serão estabelecidas em um aviso de privacidade do funcionário e notificações adicionais, conforme requerido pela lei de proteção de dados. Onde aplicável, os avisos de privacidade do funcionário serão fornecidos aos novos funcionários durante o período de integração, e uma cópia do aviso de privacidade será publicada on-line, sempre que possível, e disponível através dos contatos do setor local de Recursos Humanos. Os funcionários serão notificados e receberão uma cópia dos avisos aplicáveis de privacidade do funcionário sempre que forem feitas mudanças substanciais.

Para os clientes, prestadores de serviço e outros terceiros relevantes, um aviso de privacidade deve ser fornecido ou disponibilizado de forma recuperável e facilmente acessível, onde praticável no momento da coleta dos dados pessoais ou o mais rápido possível após.

Base legal de processamento

Os dados pessoais apenas podem ser coletados e processados pela Crawford em conformidade com as leis aplicáveis de proteção de dados e onde requerido com o consentimento do titular dos dados. Ao agir como processador de dados, os dados pessoais apenas serão processados conforme necessário para executar os serviços conforme orientado pelos

clientes, ou onde, de outra forma, for exigido pela legislação aplicável.

Sempre que o processamento dos dados pessoais estiver baseado no consentimento explícito do titular dos dados, um registro de tal consentimento precisa ser feito e mantido.

Os dados pessoais sujeitos às leis de proteção de dados da UE apenas podem ser processados em cumprimento a bases legais específicas conforme a lei. Onde a Crawford é a controladora de dados, ela é responsável por assegurar que o processamento seja conduzido segundo uma mais bases legais específicas (por exemplo, consentimento, necessário para celebrar contrato com pessoas físicas, propósitos legal legítimo, exigido por lei, necessário para defender direitos) e onde a base legal tenha sido divulgada os titulares dos dados no aviso de privacidade relevante.

Manutenção de dados

A Crawford manterá registros precisos de suas atividades de processamento, incluindo registros obrigatórios conforme estabelecido nas leis aplicáveis de proteção de dados. O Escritório de Privacidade Global mantém um inventário/registro de processamento do processamento de dados pessoais da Crawford conforme exigido pelas leis de proteção de dados da UE. O chefe de proteção de dados do grupo da UE tem a responsabilidade de assegurar que o registro do processamento seja atualizado conforme apropriado.

Direitos do titular dos dados

Os titulares dos dados têm direitos específicos relacionados a seus dados pessoais e o modo pelo qual eles são processados. Os titulares dos dados terão um mecanismo razoável para lhes permitir acessar seus dados pessoais, exercer qualquer outro direito aplicável, tais como o direito de atualizar, retificar, eliminar ou transmitir em forma portátil seus dados pessoais, se apropriado ou requerido pela lei (“Direitos do Titular dos dados”), e fazer uma consulta ou reclamação relacionada ao processamento de seus dados pessoais.

Processador de dados

Ao agir como processador de dados, a Crawford, em cumprimento às leis aplicáveis e requisitos contratuais, notificará o controlador de dados de qualquer solicitação feita pelo titular dos dados para exercer os direitos de titular dos dados e fornecer assistência razoável após solicitação para permitir que o controlador de dados responda à solicitação conforme requerido pelas leis de proteção de dados.

Controlador de dados

Ao agir como processador de dados, a Crawford tem a responsabilidade de respeitar os direitos do titular dos dados e responder a solicitações relacionadas conforme exigido pelas leis de proteção de dados. Diretor de privacidade ou um delegado fornecerá diretrizes para responder a tais solicitações; todo pessoal é responsável em seguir tais diretrizes.

Transferências internacionais de dados pessoais

Leis aplicáveis de proteção de dados e compromissos com o cliente podem exigir que a Crawford tome medidas para proteger os dados pessoais antes de os transferir para fora do país onde foram coletados.

Proteção equivalente.

A Crawford precisa tomar medidas para assegurar que as transferências internacionais de dados pessoais estejam sujeitas às salvaguardas adequadas. Os dados pessoais que forem transferidos internacionalmente precisam ser processados pela Crawford ou em nome dela conforme as leis aplicáveis de proteção de dados e compromissos do cliente.

Transferências restritas

As transferências restritas de dados pessoais precisam ser feitas segundo as leis aplicáveis de proteção de dados e compromissos do cliente.

A fim de processar adequadamente tais dados pessoais, a Crawford adotou várias medidas para assegurar que eles sejam adequadamente protegidos ao serem transferidos para fora da jurisdição de onde foram coletados.

Onde houver uma transferência restrita de dados pessoais, proteções pertinentes precisam ser utilizadas, dentre elas, a execução das cláusulas contratuais padrão onde relevante. A Crawford avaliará a necessidade de qualquer autorização relevante pelas autoridades supervisoras ou clientes.

Transferências entre o Grupo Crawford

A Crawford celebrou um Acordo de Processamento Intergrupal de dados, que incorpora as cláusulas contratuais padrão, a fim de fornecer proteções pertinentes para transferências restritas entre as entidades do grupo Crawford, bem como outro processamento de dados pessoais por uma ou mais entidade do grupo Crawford em nome de uma ou mais entidade do grupo Crawford.

Cada entidade do grupo Crawford assinará o Acordo de Transferência Intergrupal de dados, e cumprirá com ele em relação a toda transferência ou processamento entre as entidades do grupo Crawford. À medida que novas entidades fazem parte da Crawford, cada nova entidade deverá assinar o Acordo de Transferência Intergrupal de dados.

Transferências a prestadores de serviço

Antes que qualquer transferência restrita a um prestador de serviços ocorra,

a Crawford tomará medidas para incorporar as cláusulas contratuais padrão no acordo contratual aplicável entre a Crawford e o prestador.

Gestão de terceiros e prestadores de serviço

Relacionamentos comerciais com terceiros e com sua contratação precisam ser conduzidos de maneira que cumpra com esta Política e as leis aplicáveis de proteção de dados e compromissos com o cliente.

Prestadores de serviço e subprocessadores apenas podem ser contratados se forem capazes de cumprir os padrões adequados e fornecer as proteções pertinentes para os dados pessoais.

Pelo menos:

- Análise detalhada adequada de todos os prestadores de serviço e subprocessadores deve ser conduzida, antes do processamento de seus dados pessoais (incluindo armazenamento e acesso), e em uma base contínua após, conforme necessário (sujeito ao programa de gestão de risco de terceiros da Crawford).
- Devem ser implementadas obrigações contratuais pertinentes com cada prestador de serviço (onde relevante), que incluem obrigações contratuais equivalentes àquelas que se aplicam à Crawford segundo seus contratos relevantes com o cliente.
- A Crawford tomará medidas para incorporar as cláusulas contratuais padrão no acordo contratual aplicável entre a Crawford e o prestador, caso haja alguma transferência restrita.
- Todas as medidas necessárias segundo as leis aplicáveis de proteção de dados e compromissos contratuais com o cliente serão cumpridos.

Prestadores de serviço e outros terceiros precisam ser avaliados, contratados e administrados segundo o programa de gestão de risco de terceiros da Crawford.

Resposta a incidentes

Controles adequados são necessários para que os incidentes de segurança que possam impactar os dados pessoais sejam detectados, relatados e administrados segundo as políticas e procedimentos estabelecidos, incluindo a Política Global de Resposta a Incidentes, e as leis aplicáveis de proteção de dados.

Quando um evento ou incidente de segurança puder impactar os dados pessoais ou indicar uma violação a esta Política, as leis de proteção de dados ou compromissos com o cliente, o Escritório Global de Privacidade pode ser imediatamente notificado.

O Escritório Global de Privacidade tem a responsabilidade de avaliar, investigar e determinar a resposta e obrigações de notificação que surgem de um evento ou incidente de privacidade, e todo o pessoal deve cooperar com e Escritório de Privacidade conforme necessário para avaliar, investigar, mitigar, relatar e resolver eventos e incidentes de privacidade. O Escritório Global de Privacidade tem autoridade absoluta para determinar se o evento ou incidente de privacidade é uma violação de dados; o pessoal não deve especular ou identificar nenhum incidente como violação de dados a menos que orientado pelo Escritório Global de Privacidade.

Onde uma violação de dados é determinada, a Crawford precisa agir prontamente para fornecer qualquer aviso necessário aos clientes relevantes, autoridades supervisórias e titulares dos dados.

Conscientização e treinamento de privacidade

Governança de privacidade e proteção de dados são essencialmente importantes para a Crawford, e sua capacidade de:

- Cumprir as leis e compromissos contratuais com os clientes
- Controlar riscos
- Manter a confiança
- Operar efetivamente
- Suportar metas estratégicas e o modelo de governança de dados

Treinamento anual

Treinamento obrigatório sobre privacidade e segurança será obrigatório para todo o pessoal, pelo menos, em caráter anual, referente à privacidade, proteção de dados e segurança da informação.

Treinamento adicional baseado na função

Pessoal com funções que envolvem administração regular de dados pessoais e aqueles com responsabilidades chave específicas dentro da estrutura de governança da privacidade receberão treinamento e recursos adicionais baseados na função.

Recursos de privacidade incorporados

Contatos de privacidade serão identificados em toda a empresa para apoiar as iniciativas de privacidade, criar consciência entre colegas e vínculo com o Escritório Global de Privacidade.

Avaliações de impacto à privacidade

É estritamente importante que as atividades e processos sejam concebidos, implementados e realizados de forma que ofereça conformidade com as leis de proteção de dados e políticas de Crawford e a integração das proteções necessárias para dados pessoais. Este é um componente chave da privacidade segundo o princípio de concepção (*vide* Princípio 7 acima).

A Crawford desenvolveu uma política e procedimentos para conduzir avaliações de impacto à privacidade, e, onde necessário, avaliações formais de impacto à proteção de dados.

Avaliações de impacto à privacidade

Avaliações de impacto da privacidade (PIA, Privacy Impact Assessments) devem ser conduzidas para avaliar o impacto à privacidade e identificar riscos relacionados aos projetos, atividades e prestadores de serviço que possam impactar a privacidade e a segurança dos dados pessoais. Antes de contratar um novo prestador de serviços, começar um novo projeto, conceber ou atualizar substancialmente um novo sistema, combinar dados de dois sistemas ou registrar configurações, ou de outra forma, envolver-se toda atividade ou processo novos ou substancialmente modificados que possam impactar os dados pessoais ou como são processados, uma PIA precisa ser conduzida.

Avaliações de impacto da proteção de dados

Onde uma PIA indicar que o processamento dos dados pessoais tem a probabilidade de resultar em um alto risco aos direitos e liberdade das pessoas, uma avaliação de impacto à proteção de dados (DPIA, Data Protection Impact Assessment) será conduzida antes de tal processamento a fim de determinar a natureza desses riscos e mitigá-los dentro do possível. Tal processamento não pode começar até que o Comitê Consultivo de Privacidade tenha determinado que os riscos do processamento foram adequadamente mitigados.

Avaliação e atualizações contínuas

Avaliações de risco contínuas de processos e sistemas administrativos serão conduzidas para:

- verificar a implementação e o cumprimento de controles internos, políticas e procedimentos; e
- identificar qualquer falha de conformidade.

Processos e procedimentos de conformidade com a privacidade serão atualizados para responder por:

- novas ameaças ou riscos aos negócios que foram identificados;

- mudanças a operações e atividades;
- mudanças na legislação de privacidade; e
- áreas para melhoria com base nos resultados das avaliações de risco, PIA, auditorias, reclamações, lições aprendidas de iniciativas de resposta a incidentes, e/ou outros meios.

Governança

Escritório Global de Privacidade (Global Privacy Office)

A Crawford estabeleceu um Escritório Global de Privacidade, concebido para desenvolver, administrar e orientar iniciativas de privacidade em toda a empresa. Em um alto nível, o Escritório Global de Privacidade:

- Inicia e incentiva uma cultura de privacidade dentro da Crawford
- Assegura que a privacidade seja incluída nos objetivos e metas da empresa
- Administra a conformidade em um ambiente regulamentar complexo

O Escritório Global de Privacidade realiza o acima mencionado com a participação e colaboração de várias funções dentro da Crawford, tais como, Jurídico, Escritório de Ética e Conformidade, Tecnologia da Informação e Segurança da Informação.

Diretor de Privacidade

O diretor de privacidade lidera o Escritório Global de Privacidade e tem responsabilidade geral pela privacidade dentro da Crawford. Isso inclui:

- Desenvolver e manter esta Política e apoiar políticas e procedimentos;
- Estabelecer a direção e as prioridades para o programa de conformidade com a privacidade, incluindo a implementação dos objetivos de privacidade em toda a empresa; e
- Gestão de orçamento e recursos (incluindo executivos de proteção de dados).

Linhas, departamentos e entidades locais de serviço global são responsáveis pela iniciação e implementação de objetivos de privacidade em toda a empresa em consulta com o diretor de privacidade.

Diretores de proteção de dados e diretores de privacidade de dados

A Crawford criou funções adicionais com responsabilidade formal pela conformidade com as leis de proteção de dados em regiões e jurisdições específicas, conforme abaixo definido. A Crawford apontará pessoas a estas funções. Estas pessoas são responsáveis perante o diretor de privacidade em relação a suas obrigações específicas de supervisionar a conformidade

com esta Política, políticas e procedimentos relacionados à proteção de dados e leis aplicáveis de proteção de dados.

União Europeia

A autoridade de proteção de dados é a função oficial exigida pela lei de proteção de dados da UE segundo certas condições. A Crawford estabelecerá uma ou mais funções de diretor de proteção de dados dentro da UE, com responsabilidade para as leis de proteção de dados da UE em uma jurisdição particular ou em nome do grupo Crawford.

- Executivo de proteção de dados do grupo. A autoridade de proteção de dados do grupo da UE é responsável pelo monitoramento e consultoria em relação à conformidade da Crawford com as leis de proteção de dados da UE, bem como auxiliar com a atualização regular dos registros obrigatórios do processamento, e dar seus comentários sobre a DPIA obrigatória. O diretor de proteção de dados do grupo da UE será um membro do Escritório Global de Privacidade, e reportará ao diretor de privacidade, porém, precisa ser capaz de exercer suas responsabilidades de maneira independente. A autoridade de proteção de dados do grupo da UE será apoiado pelos líderes de privacidade nas jurisdições relevantes da UE.
- Executivo de proteção de dados do país. A autoridade de proteção de dados de um país específico da UE pode ser nomeado interna ou externamente, e será responsável pela conformidade com a proteção de dados em uma jurisdição particular e se reportará ao gerente do país para essa jurisdição.

Cada executivo de proteção de dados da UE que é nomeado estará sujeito aos termos que garantam sua independência e imparcialidade. A função da autoridade de proteção de dados não é comercial, e ele não deve ser colocado em uma situação (por exemplo, através da atribuição de responsabilidades adicionais) que possam criar um conflito de interesses. Cada executivo de proteção de dados da UE terá independência para efetuar suas obrigações oficiais e elaborar relatórios referentes à conformidade com as leis de proteção de dados da UE para os níveis mais altos da administração conforme segue:

- A autoridade de proteção de dados do grupo da UE está habilitado a comunicar assuntos relacionados à conformidade com as leis de proteção de dados da UE à equipe de gestão executiva.
- A autoridade de proteção de dados de um país específico da UE está habilitado a comunicar questões relativas a conformidade com as leis de proteção de dados em um jurisdição particular ao gerente do país da referida jurisdição.

Um registro atualizado dos indicados da autoridade de proteção de dados da UE será mantido pelo Escritório de Privacidade, e também deve ser divulgado em avisos de privacidade relevantes do titular dos dados, e notificado às autoridades de supervisão pertinentes, conforme exigido pelas leis aplicáveis de proteção de dados da UE.

As Filipinas

A autoridade de proteção de dados das Filipinas é necessário para cada entidade da Crawford das Filipinas. A autoridade de proteção de dados das Filipinas pode ser nomeado para uma ou mais entidades das Filipinas, e será responsável por supervisionar a conformidade com as leis de proteção de dados das Filipinas e enviar todo registro segundo as leis aplicáveis de proteção de dados para a Comissão Nacional de Privacidade das Filipinas. Um diretor de Conformidade para cada entidade das Filipinas pode ser nomeado para assistir o diretor de proteção de dados das Filipinas. O diretor de proteção de dados atual para cada entidade das Filipinas será notificado à Comissão Nacional de Privacidade das Filipinas.

Canadá

A autoridade de privacidade de dados do Canadá será nomeado para uma ou mais entidades canadenses segundo as leis de proteção de dados do Canadá, e será responsável por supervisionar a conformidade com as leis canadenses de proteção de dados.

Outras jurisdições

Onde requerido pelas leis aplicáveis de proteção de dados, a Crawford atribuirá funções adicionais com responsabilidade formal para proteção da privacidade e dados em jurisdições particulares, que terão responsabilidades perante o diretor de privacidade em relação a suas obrigações relevantes de supervisionar a conformidade com a privacidade.

Líderes de privacidade na UE

Um líder de privacidade será nomeado para cada entidade da Crawford da União Europeia para apoiar o diretor de proteção de dados do grupo da UE no recebimento, revisão e resposta a consultas e reclamações de clientes, titulares dos dados e autoridades supervisórias, e condução de toda DPIA necessária.

Coordenadores de privacidade

A menos que uma exceção seja concedida pelo Escritório Global de Privacidade, cada afiliado e cada departamento global atribuirá um coordenador de privacidade, responsável por ser um ponto compartilhado de contato entre o Escritório Global de Privacidade e sua entidade ou departamento, e por identificar questões de conformidade no local e encaminhá-las ao Escritório Global de Privacidade, e auxiliá-lo na

implementação de iniciativas de privacidade. Os coordenadores de privacidade são responsáveis perante o diretor de privacidade em relação às suas obrigações relevantes.

Um líder de privacidade da UE também pode prestar serviço como coordenador de privacidade.

Comitê Consultivo de Privacidade

O Comitê Consultivo de Privacidade é um grupo sênior e interfuncional estabelecido para discutir questões de conformidade e gestão de proteção de dados que autorizem um exame ou decisão interfuncional. O Comitê Consultivo de Privacidade é liderado pelo diretor de privacidade, e a associação inclui todos os diretores de proteção de dados e diretores de privacidade de dados, bem como representantes dos principais departamentos, incluindo o Escritório de Ética e Conformidade, Jurídico, Tecnologia da Informação e Segurança da Informação.

O Comitê se reúne, pelo menos, em uma base trimestral e reporta-se à equipe de gestão executiva global. O Comitê preparará um relatório anual para ser apresentado ao Conselho de Diretores da Crawford, ou comitê designado, resumindo eventos significativos durante o ano civil anterior (por exemplo, marcos alcançados).

O Comitê Consultivo de Privacidade tem autorização expressa de levantar junto à equipe de gestão executiva global e, onde apropriado, o Conselho de Diretores da Crawford (ou comitê designado) em uma base ad-hoc, questões ou comentários relacionados aos projetos potencialmente de alto risco ou possíveis instâncias de não conformidade relevante.

Definições

"**Cliente**" significa um cliente atual, anterior ou potencial da Crawford, e qualquer outra parte em cujo nome a Crawford age segundo orientação de tal cliente.

"**Dados pessoais dos clientes**" significa dados pessoais que a Crawford processa (como processador de dados) em nome de seus clientes.

"**Controlador de dados**" ou "**Controlador**" significa a pessoa/entidade natural ou jurídica que sozinha ou em conjunto com outros, determina os propósitos e meios do processamento de dados pessoais.

"**Processador de dados**" ou "**Processador**" significa a pessoa/entidade natural ou jurídica que processa dados pessoais em nome do controlador.

"**Leis de proteção de dados**" significa, na medida do que se aplica à Crawford, as leis, normas e regulamentações referentes à proteção da privacidade ou dos dados, ou de outra forma, que regem o processamento

dos dados pessoais (incluindo as leis de proteção dos dados na UE).

"**Titular dos dados**" significa a pessoa física a quem os dados pessoais se referem.

"**EEE**" significa Espaço Econômico Europeu.

"**Leis de proteção de dados da UE**" significa a Diretiva da UE 95/46/EC, conforme transposto à legislação nacional de cada Estado Membro e conforme emenda, substituição ou revogação esporádica, incluindo pela Regulamentação Geral de Proteção de dados da UE 2016/679 ("GDPR") e leis que implementam ou complementam o GDPR, bem como toda legislação sucessora de proteção de dados do Reino Unido ao GDPR adotada se o Reino Unido sair da União Europeia.

"**Dados pessoais**" significa toda informação relacionada a uma pessoa natural identificada ou identificável; inclui informações em qualquer formato ou meio, independentemente de a informação estar criptografada ou não. Uma pessoa pode ser diretamente identificada por seu nome, endereço, ID de funcionário, número de reclamação, endereço de e-mail, número de telefone ou identificador do governo, por exemplo. Uma pessoa pode ser indiretamente identificada por meio de vinculação ou combinação de informações adicionais que podem ou não estar sob custódia ou controle da Crawford, tais como um endereço de IP, endereço MAC, identificador de dispositivo, identificador biométrico ou outro identificador exclusivo, informações de geolocalização, informações genéticas ou de DNA, por exemplo.

"**Violação de dados**" significa todo acesso não autorizado conhecido ou razoavelmente suspeito, uso, divulgação ou outro processamento de dados pessoais, bem como toda perda, roubo ou aquisição de dados pessoais ou qualquer incidente que comprometa a segurança dos dados pessoais.

"**Pessoal**" significa todos os funcionários que trabalham em período integral, em meio período, temporários, regulares e terceirizados, consultores e trabalhadores sem vínculo empregatício.

"**Processo**" significa toda operação ou conjunto de operações executadas em dados pessoais ou conjunto destes, seja por meios automatizados ou não, tais como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou outra forma de disponibilização, alinhamento ou combinação, restrição, eliminação ou destruição dos dados.

"**Transferência restrita**" significa uma transferência de dados pessoais pela, entre ou para a Crawford (incluindo toda empresa do grupo Crawford) entre fronteiras nacionais, que é proibida pelas leis aplicáveis de proteção de dados ou acordos com o cliente, na falta de cláusulas contratuais padrão.

"**Dados confidenciais**" significa dados pessoais considerados confidenciais ou que, de outra forma, estão sujeitos a normas regulamentares mais estritas segundo as leis de proteção de dados (incluindo "categorias especiais de dados pessoais" conforme as leis de proteção de dados da UE), e dados pessoais que, se acessados ou divulgados sem autorização, poderiam levar a roubo de identidade ou dano substancial financeiro, físico ou à reputação, incluindo também: raça ou etnia; crenças religiosas ou filosóficas; associação a sindicatos; afiliação política; orientação sexual ou vida privada; informações de saúde, tratamento médico; informações sobre deficiência física ou mental; informações de saúde protegidas; saúde mental; genética, biometria; números de cartão de crédito ou contas financeiras; dados de cartão de pagamento; número de CPF ou identificadores do governo; relatório de crédito ou verificação de antecedentes; e antecedentes criminais ou processos penais.

"**Cláusulas Contratuais Padrões**" significa:

(a) para dados pessoais sujeitos às leis de proteção de dados da UE, as cláusulas contratuais padrão da UE para a transferência de dados pessoais a processadores localizados em terceiros países ou todo mecanismo de transferência de dados sucessor inerente ou alternativo, reconhecido pela Comissão Europeia segundo o GDPR (Artigos 44-46); e/ou

(b) para dados pessoais sujeitos às leis de proteção de dados, além das leis de proteção de dados da UE, outras leis nacionais equivalentes estabelecidas para assegurar proteção adequada para transferências internacionais de dados pessoais.

"**Subprocessador**" significa um prestador de serviços nomeado por ou em nome de uma entidade da Crawford (em sua capacidade como processador de dados) que processará dados pessoais do cliente.

"**Autoridade supervisória**" significa a autoridade regulamentar relevante com relação às leis de proteção de dados, incluindo a autoridade supervisória conforme definido nas leis de proteção de dados da UE.

"Prestador de serviços" significa um processador de dados terceirizado (incluindo um subprocessador) que fornece mercadorias ou serviços para uma entidade da Crawford ou para outra entidade ou pessoa em nome de uma entidade da Crawford.

Contato

O responsável por esta Política é o diretor de privacidade. Para outras informações, entre em contato com o Escritório Global de Privacidade (Global Privacy Office) (privacy@global.crawco.com).

Informações sobre o documento

Nome do documento	Política Global de Privacidade e Proteção de dados
Categoria	Política global
Política e Documentos Correlatos	Política de Gestão de dados Pessoais Política de Gestão de Risco de Terceiros Política Global de Resposta a Incidentes Política de Gestão de Registros e Informações Código de ética e conduta empresarial
Aprovada por	Elizabeth Alaniz, diretora de privacidade
N.º da versão — data de vigência	1.0 - Maio de 2018