POLÍTICA DE PROTEÇÃO DE DADOS E DE PRIVACIDADE

Aplicação Móvel IBC Security (Cliente)

Versão 1.0

[DATA A DEFINIR]

IBC SECURITY, LDA

Alvarás de Segurança Privada: 171-A / 171-C

NIF: 507 737 520

IBC SECURITY, LDA, sociedade comercial com sede na Urbanização Quinta Verde, Rua Mar, Lote 2, Sítio das Areias, 8135-171 Almancil, pessoa coletiva n.º 507737520, registada sob este mesmo número na Conservatória do Registo Comercial de Faro, detentora dos Alvarás de Segurança Privada n.º 171-A e 171-C emitidos pela Polícia de Segurança Pública; a **"IBC SECURITY"**, pauta-se pelo respeito total da sua privacidade e valoriza a relação que mantém consigo.

A presente Política de Proteção de Dados e de Privacidade tem como objetivo expor de uma forma clara e concisa como a **IBC SECURITY** trata os seus Dados Pessoais no contexto da utilização da aplicação móvel IBC Security para clientes (adiante designada "Aplicação" ou "App"), disponível para dispositivos Android e iOS, e garante a privacidade dos seus dados.

A Aplicação constitui uma ferramenta digital complementar aos serviços de segurança privada prestados pela IBC SECURITY, permitindo ao Cliente e aos membros da sua família autorizados aceder a funcionalidades relacionadas com o serviço de segurança contratado, incluindo:

a) Criação e gestão de conta de utilizador;
b) Utilização da funcionalidade de alerta de emergência (SOS);
c) Gestão do perfil pessoal e contactos de emergência;
d) Registo e gestão de membros da família;
e) Receção de notificações de serviço;
f) Pedidos técnicos e comerciais;
g) Consulta de faturas e documentação contratual.

1. Responsável pelo tratamento dos seus Dados Pessoais

A **IBC SECURITY** é entidade Responsável pelo Tratamento dos seus Dados Pessoais recolhidos através da Aplicação, determinando para o efeito, sem limitar:

- os Dados Pessoais que devem ser tratados no contexto da utilização da Aplicação e da prestação de serviços de segurança privada;
- as Finalidades para as quais os seus Dados Pessoais são tratados; e,
- os meios a aplicar para o tratamento dos seus Dados Pessoais.

2. Princípios aplicáveis à proteção dos seus Dados Pessoais

O Tratamento dos seus Dados Pessoais é efetuado de acordo com os princípios gerais enunciados no Regulamento Geral sobre a Proteção de Dados ("RGPD"), nomeadamente:

- No contexto da relação consigo, a **IBC SECURITY** assegura que os seus Dados Pessoais serão tratados de forma lícita, leal e transparente (**«Princípio da licitude, lealdade e transparência»**);
- A **IBC SECURITY** recolhe os seus Dados Pessoais para finalidades determinadas, explícitas e legítimas e não trata posteriormente os mesmos Dados de uma forma incompatível com essas finalidades (**«Princípio da limitação das finalidades»**);
- A **IBC SECURITY** assegura que apenas são tratados os Dados Pessoais adequados, pertinentes e limitados ao estritamente necessário às finalidades para as quais são tratados (**«Princípio da minimização dos dados»**);
- A **IBC SECURITY** adota as medidas adequadas para que os Dados Pessoais inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (**«Princípio da exatidão»**);
- A **IBC SECURITY** conserva os Dados Pessoais de forma que permita a sua identificação apenas durante o período necessário para as finalidades para as quais são tratados (**«Princípio da conservação»**);
- A **IBC SECURITY** assegura que os seus Dados Pessoais são tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (**«Princípio da integridade e confidencialidade»**).

Adicionalmente, a **IBC SECURITY** procede ao tratamento dos seus dados através da aplicação de medidas técnicas e organizativas que assegurem a Proteção de Dados desde a Conceção e por Defeito, para que os seus Dados Pessoais sejam tratados de acordo com as melhores práticas desde o momento da sua recolha até à sua destruição.

3. Dados Pessoais, Tratamento de Dados Pessoais e Titular dos Dados

Dados Pessoais são todas as informações e/ou elementos que, independentemente do seu suporte, o podem identificar ou tornar identificável, direta ou indiretamente, perante a **IBC SECURITY**, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, os seus dados de localização e/ou identificadores por via eletrónica ou a um ou mais elementos específicos da sua identidade física, fisiológica, genética, mental, económica, cultural ou social.

Tratamento de Dados Pessoais significa a operação ou conjunto de operações efetuadas sobre Dados Pessoais dos Titulares dos Dados, através de meios automatizados ou não-automatizados, desde a recolha da informação até à sua destruição.

No contexto da Aplicação, o **Titular dos Dados** é o cliente da IBC SECURITY que mantenha uma relação contratual ativa de prestação de serviços de segurança privada, bem como os respetivos membros da família previamente autorizados pelo titular da conta.

A **IBC SECURITY** não solicita ou recolhe voluntária ou diretamente dados pessoais de menores de idade através da Aplicação. Se a **IBC SECURITY** descobrir que recolheu inadvertidamente dados pessoais de um menor de 18 anos, procederá imediatamente à eliminação dos registos com os dados pessoais desse menor (ver secção 16).

4. Categoria de Dados Pessoais que a IBC SECURITY trata na Aplicação

No contexto da utilização da Aplicação, a **IBC SECURITY** procede ao tratamento das seguintes categorias de Dados Pessoais:

4.1. Dados fornecidos diretamente pelo utilizador

Categoria de Dados Pessoais	Dados Pessoais
Dados de identificação pessoal	Nome completo
Dados de contacto pessoais	Endereço de email, números de telefone (principal e secundário)
Dados de morada	Endereço da propriedade protegida, nome da propriedade
Dados de contactos de emergência	Nome, telefone(s) e notas de até 3 contactos de emergência designados pelo titular
Dados das credenciais de segurança	Email e palavra-passe (encriptada), PIN de acesso (encriptado localmente no dispositivo)

4.2. Dados recolhidos automaticamente

Categoria de Dados Pessoais	Dados Pessoais
Dados de notificação	Identificador FCM (Firebase Cloud Messaging) para envio de notificações push
Dados do dispositivo	Sistema operativo (Android/iOS), plataforma
Dados de autenticação	Identificador de utilizador (UID), sessões de autenticação

4.3. Dados recolhidos mediante consentimento específico

Categoria	Dados Pessoais	Condições de Recolha
Dados de localização geográfica	Coordenadas GPS (latitude, longitude), precisão em metros, marca temporal	Recolhida apenas no momento exato do acionamento de um alerta SOS, e apenas se todas as seguintes condições estiverem reunidas: (1) o serviço IBC Guardian One Premium estiver ativo;

		(2) o serviço de localização estiver ativado pela IBC SECURITY; (3) o utilizador tiver aceite explicitamente a partilha de localização

Nota importante sobre localização: A **IBC SECURITY não** realiza rastreamento contínuo ou periódico da localização dos seus clientes. A localização é obtida **exclusivamente** no momento do acionamento de um alerta SOS e utilizada unicamente para efeitos de resposta à emergência.

4.4. Dados de membros da família

Categoria de Dados Pessoais	Dados Pessoais
Dados de identificação	Nome completo, grau de parentesco
Dados de contacto	Email, telefone(s), notas
Dados das credenciais de segurança	Email e palavra-passe (encriptada)
Dados de preferências	Idioma da aplicação (Português, English, Français, Español, Deutsch)
Dados de permissões	Acesso a SOS, código de alarme, pedidos técnicos/comerciais, faturas

5. Finalidades para o tratamento dos seus Dados Pessoais

Finalidades	Finalidades de Tratamento
Gestão da conta e perfil	Gestão de clientes para a prestação de serviços de segurança privada, autenticação e controlo de acessos à Aplicação
Alertas SOS e resposta a emergências	Receção e processamento de alertas de emergência, despacho de equipas de intervenção rápida, monitorização pela Central de Segurança (Guardian One)
Geolocalização em emergência	Localização do cliente no momento exato do alerta SOS para despacho imediato de equipa ao local (apenas mediante consentimento explícito)
Gestão de contactos de emergência	Manutenção de contactos designados pelo cliente para situações de emergência
Gestão de membros da família	Registo e gestão de contas de familiares autorizados pelo titular
Notificações de serviço	Envio de notificações push relativas a alertas, faturas, comunicações operacionais
Gestão de pedidos	Processamento de pedidos técnicos e comerciais submetidos pelo cliente
Gestão de faturação	Disponibilização e consulta de faturas e documentação contratual

Segurança da conta	Proteção contra acessos não autorizados através de PIN, biometria e bloqueio automático

6. Fundamentos de Licitude

Por referência ao «Princípio da Licitude» consagrado nas leis de proteção de dados vigentes e futuras, a **IBC SECURITY** só trata os seus Dados Pessoais quando existir um fundamento de licitude que legitime o tratamento:

Fundamentos de Licitude	Em que é que consistem?	Aplicação na App
Consentimento (Art. 6.º, n.º 1, al. a) RGPD)	A IBC SECURITY só tratará os seus Dados Pessoais se consentir no respetivo Tratamento através de uma manifestação de vontade, livre, específica, informada e explícita.	Localização GPS em alertas SOS; extensão do serviço a membros da família
Execução do contrato (Art. 6.º, n.º 1, al. b) RGPD)	A IBC SECURITY poderá tratar dos seus Dados Pessoais se os mesmos forem necessários para a execução de um contrato de prestação de serviços de segurança privada.	Gestão da conta e perfil, alertas SOS, notificações push, contactos de emergência, faturação
Cumprimento de obrigação jurídica (Art. 6.º, n.º 1, al. c) RGPD)	A IBC SECURITY poderá tratar os seus Dados Pessoais para assegurar e garantir o cumprimento de obrigações jurídicas a que esteja sujeita.	Conservação de faturas e documentação fiscal
Defesa de interesses vitais (Art. 6.º, n.º 1, al. d) RGPD)	A IBC SECURITY poderá tratar os seus Dados Pessoais para assegurar a defesa dos seus interesses vitais, designadamente quando essencial à sua vida.	Alertas SOS e resposta a emergências, contactos de emergência
Interesses Legítimos (Art. 6.º, n.º 1, al. f) RGPD)	A IBC SECURITY poderá tratar os seus Dados Pessoais desde que esse mesmo Tratamento não prevaleça sobre os seus interesses ou direitos e liberdades fundamentais.	Segurança da conta (PIN, biometria), registos de auditoria

7. Prazo de conservação dos seus Dados Pessoais

A **IBC SECURITY** conserva os seus Dados Pessoais apenas pelo período de tempo necessário à execução das finalidades específicas para as quais foram recolhidos. No entanto, a **IBC SECURITY** pode ser obrigada a conservar alguns Dados Pessoais por um período mais longo, tomando em consideração fatores como:

- Obrigações legais de conservar Dados Pessoais por um determinado período;
- Prazos de prescrição, ao abrigo das leis em vigor;
- Litígios (eventuais); e,
- Orientações emitidas pelas autoridades de proteção de dados competentes.

Categoria de Dados	Período de Conservação	Fundamento
Dados da conta (nome, contactos, morada)	Durante a vigência do contrato + período legalmente exigido após cessação	Obrigações contratuais e legais
Alertas SOS (incluindo localização)	Período definido pela legislação aplicável ao setor de segurança privada	Obrigações legais, necessidade probatória
Contactos de emergência	Durante a vigência do contrato	Execução do contrato
Membros da família	Durante a vigência do contrato ou até revogação pelo titular	Consentimento e execução do contrato
Tokens FCM (notificações)	Até logout, desinstalação da app ou invalidação automática	Necessidade técnica
Faturas e documentação fiscal	10 anos (Art. 40.º do Código Comercial, Art. 123.º do CIRC)	Obrigação legal
Registos de auditoria	Período definido pela legislação aplicável	Interesse legítimo e obrigação legal

8. Partilha dos seus Dados Pessoais

Entidades	Porque partilhamos os seus Dados Pessoais
Central de Segurança (Control Room)	Os seus dados são acedidos pela Central de Segurança para gestão operacional do serviço de segurança contratado.
IBC Guardian One	Os seus dados são acedidos pela plataforma de monitorização de emergências para receção e tratamento de alertas SOS.
Equipas de Intervenção Rápida	Os seus dados são transmitidos via despacho para intervenção no local em caso de alarme ou emergência.
Administração	Todos os dados da conta são acedidos para gestão contratual e faturação.
Subcontratantes	Os seus Dados Pessoais podem ser partilhados com empresas encarregues da prestação de serviços, vinculadas por contrato escrito (DPA).

Autoridades competentes	Em cumprimento de obrigações legais, os Dados Pessoais poderão ser transmitidos a autoridades judiciais, administrativas (PSP, GNR), de supervisão ou regulatórias.

Subcontratantes específicos:

Prestador	Serviço	Localização	Garantias
Google LLC (Firebase)	Autenticação, base de dados, armazenamento, notificações push	UE (europe-west1)	DPA Google Cloud, SCCs, ISO 27001
Google LLC (FCM)	Serviço de notificações push	UE/EUA	DPA Google Cloud, EU-US Data Privacy Framework

9. Transferências Internacionais de Dados Pessoais

Os dados pessoais são armazenados primariamente em servidores localizados na **União Europeia** (região europe-west1 da Google Cloud).

A **IBC SECURITY** pode transferir os seus Dados Pessoais para fora do Espaço Económico Europeu ("EEE"), na medida em que determinados serviços da Google possam envolver processamento fora do EEE. Contudo, a **IBC SECURITY** apenas transfere os seus Dados Pessoais para fora do EEE:

- Quando a transferência for feita para uma localização que a Comissão Europeia considere garantir a proteção adequada;
- Quando tiver implementado cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia;
- Ao abrigo do EU-US Data Privacy Framework (quando aplicável); ou,
- Quando a lei autorizar essa transferência, por exemplo, para a defesa de um direito num processo judicial.

Poderá solicitar informação detalhada sobre as medidas de segurança através do email **dpo@rgpdconsultores.pt**.

10. Os seus direitos e como exercê-los

Na qualidade de Titular dos Dados Pessoais tratados pela **IBC SECURITY** através da Aplicação, tem os seguintes direitos:

Direitos	Em que consistem?
Direito à prestação de informação	Tem o direito de obter informações claras, transparentes e facilmente compreensíveis sobre como a IBC SECURITY usa os seus Dados Pessoais.
Direito de acesso (Art. 15.º)	Tem o direito de obter informação sobre que Dados Pessoais a IBC SECURITY trata e como são tratados.
Direito de retificação (Art. 16.º)	Se os seus Dados estiverem incorretos ou incompletos, poderá pedir para a IBC SECURITY os corrigir.
Direito ao apagamento (Art. 17.º)	Permite solicitar o apagamento dos seus dados, desde que não existam fundamentos válidos para que a IBC SECURITY continue a usá-los.
Direito à limitação do tratamento (Art. 18.º)	Tem o direito de "bloquear" ou impedir o uso futuro dos seus Dados enquanto a IBC SECURITY avalia um pedido.
Direito à portabilidade (Art. 20.º)	Tem o direito de obter e reutilizar determinados Dados Pessoais para os seus próprios fins.
Direito à oposição (Art. 21.º)	Tem o direito de se opor a determinados tipos de tratamento, por motivos relacionados com a sua situação particular.
Direito de apresentar queixa	Junto da CNPD (www.cnpd.pt, Av. D. Carlos I, 134, 1.º, 1200-651 Lisboa, geral@cnpd.pt).
Direito de revogação do consentimento	Tem o direito de retirar o consentimento a qualquer momento, sem comprometer a licitude do tratamento anterior.

Poderá exercer os seus direitos através dos seguintes meios:

- **Email:** rgpd@ibcsecurity.com
- **Email do DPO:** dpo@rgpdconsultores.pt
- **Correio postal:** IBC Security, Lda. — Encarregado de Proteção de Dados, Urb. Quinta Verde, Rua do Mar, Lote 2, 8135-171 Almancil, Portugal

A **IBC SECURITY** responderá aos pedidos no prazo máximo de **30 dias** a contar da receção, podendo este prazo ser prorrogado por mais 60 dias em casos de complexidade.

11. O Encarregado de Proteção de Dados

A **IBC SECURITY** procedeu à nomeação de um encarregado da proteção de dados pessoais, o qual assume uma função fundamental no acompanhamento das atividades de tratamento de dados realizadas e na garantia da respetiva conformidade legal.

O Encarregado de Proteção de Dados tem as seguintes funções:

1. Controlar a conformidade dos tratamentos realizados pela IBC SECURITY com as disposições das leis de proteção de dados;
2. Prestar aconselhamento à IBC SECURITY;
3. Cooperar com as Autoridades de Controlo (CNPD); e,
4. Constituir um ponto de contacto com as Autoridades de Controlo e com os titulares de dados.

Poderá contactar o encarregado de proteção de dados através do email **dpo@rgpdconsultores.pt**.

12. Segurança dos seus Dados Pessoais

12.1. Medidas técnicas específicas da Aplicação

- **Encriptação em trânsito:** Todas as comunicações utilizam protocolo TLS;
- **Encriptação em repouso:** Os dados armazenados no Firebase são encriptados em repouso;
- **Autenticação segura:** Política de palavra-passe forte (mínimo 12 caracteres);
- **PIN encriptado:** Armazenado de forma encriptada no dispositivo (Keychain/Keystore);
- **Bloqueio biométrico:** Bloqueio automático quando a Aplicação entra em segundo plano;
- **Tokens de autenticação:** Renovação automática com validação contínua;
- **Regras de acesso:** Cada cliente acede exclusivamente aos seus próprios dados;
- **Limpeza automática de tokens:** Tokens inválidos são automaticamente removidos.

12.2. Medidas organizativas

- **Princípio do privilégio mínimo:** Cada operador acede apenas aos dados necessários;
- **Registo de acessos:** Todas as ações são registadas em log de auditoria;
- **Formação:** Operadores recebem formação sobre proteção de dados e sigilo profissional;
- **Sigilo profissional:** Colaboradores vinculados nos termos da Lei n.º 34/2013;
- **Cópias de segurança:** Backups diários com retenção de 14 dias, na UE;
- **Gestão de incidentes:** Notificação à CNPD no prazo de 72 horas quando aplicável.

13. Confidencialidade

A **IBC SECURITY** reconhece que a informação que nos fornece pode ser confidencial. A **IBC SECURITY** não vende, aluga, distribui, nem disponibiliza comercialmente os Dados Pessoais a nenhuma entidade terceira,

exceto nos casos em que necessita partilhar informação com os Prestadores de Serviço para os fins estabelecidos nesta Política.

14. Funcionalidade SOS — Alerta de Emergência

14.1. Acesso Rápido (Quick Access)

A Aplicação disponibiliza um botão de **Acesso Rápido SOS** que permite acionar um alerta de emergência **sem necessidade de autenticação prévia** (login). Esta funcionalidade foi desenhada para garantir que, em situação de perigo iminente, o utilizador possa solicitar ajuda de forma imediata.

14.2. Dados transmitidos no alerta SOS

Quando um alerta SOS é acionado, os seguintes dados são transmitidos para a Central de Segurança:

- Identificação do cliente (nome, número de cliente);
- Número de telefone e email associados à conta;
- Tipo de alerta (acesso rápido, via aplicação, ou via membro da família);
- Marca temporal do alerta;
- Localização GPS (apenas com serviço Premium ativo e consentimento explícito);
- Plataforma do dispositivo (Android/iOS).

14.3. Destinatários do alerta SOS

- **IBC Guardian One** — Plataforma de monitorização de emergências;
- **Equipas de Intervenção Rápida (Fast Response)** — Operadores de campo;
- **Operadores da Central de Segurança (Control Room)** — Coordenação da resposta.

14.4. Proteção contra acionamentos involuntários

A Aplicação implementa um mecanismo de segurança (slider deslizante) e um período mínimo de 60 segundos entre alertas consecutivos.

15. Dados Biométricos

A Aplicação oferece autenticação biométrica (impressão digital ou reconhecimento facial). Estes dados biométricos são:

- Processados **exclusivamente no dispositivo** do utilizador;
- **Nunca transmitidos** para servidores da IBC SECURITY, Firebase ou terceiros;
- **Nunca armazenados** pela Aplicação — apenas o resultado da verificação é utilizado.

A **IBC SECURITY** não tem acesso, em momento algum, aos dados biométricos do utilizador.

16. Utilização por Menores

A Aplicação não se destina a menores de 18 anos. Nos termos da Lei n.º 58/2019, o tratamento de dados pessoais de menores com idade inferior a 13 anos requer o consentimento dos respetivos representantes legais.

17. Notificações Push

A Aplicação utiliza Firebase Cloud Messaging (FCM) para envio de notificações relativas a alertas de segurança, faturas e comunicações de serviço.

As notificações podem ser **desativadas a qualquer momento** nas definições do dispositivo. A desativação **não afeta** o funcionamento da funcionalidade SOS.

18. Contactos

IBC SECURITY, LDA

Urbanização Quinta Verde, Rua Mar, Lote 2, Sítio das Areias, 8135-171 Almancil

Alvarás de Segurança Privada: 171-A / 171-C

NIF: 507 737 520

Email para exercício de direitos: **rgpd@ibcsecurity.com**

Email do Encarregado de Proteção de Dados: **dpo@rgpdconsultores.pt**

19. Alterações a esta Política

A **IBC SECURITY** poderá atualizar periodicamente a presente Política. Quaisquer alterações significativas serão comunicadas através de notificação na Aplicação e/ou email.

20. Legislação Aplicável

- **Regulamento (UE) 2016/679** — Regulamento Geral sobre a Proteção de Dados (RGPD);
- **Lei n.º 58/2019, de 8 de agosto** — Execução do RGPD na ordem jurídica portuguesa;
- **Lei n.º 34/2013, de 16 de maio** — Regime da atividade de segurança privada;
- **Portaria n.º 273/2013, de 20 de agosto** — Regulamentação da Lei n.º 34/2013.

A presente Política foi redigida em conformidade com o RGPD, a Lei n.º 58/2019 e as orientações da CNPD.