Política de Proteção de Dados e de Privacidade — Aplicação Móvel IBC Security (Colaborador)

Última atualização: [DATA A DEFINIR] **Versão:** 1.0

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"**, na qualidade de entidade empregadora, pauta-se pelo respeito total da privacidade dos seus colaboradores e pelo cumprimento integral das obrigações em matéria de proteção de dados pessoais.

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 Dados Pessoais dos seus colaboradores no contexto da utilização da aplicação móvel IBC Security para colaboradores (adiante designada "Aplicação" ou "App"), disponível para dispositivos Android e iOS.

A Aplicação constitui uma ferramenta digital de gestão interna da relação laboral, disponibilizada pela **IBC SECURITY** aos seus colaboradores com contrato de trabalho ativo, permitindo o acesso a funcionalidades relacionadas com a execução da sua prestação profissional, incluindo:

a) Consulta de recibos de vencimento; b) Consulta de escalas de trabalho; c) Receção de comunicados e procedimentos internos; d) Submissão de pedidos de férias e consulta de mapa de férias; e) Submissão de folhas de ponto mensais; f) Upload e gestão de documentação profissional obrigatória; g) Gestão de contactos de emergência; h) Receção de notificações push de serviço.

Para que fique totalmente esclarecido e possa contactar-nos para saber quaisquer informações adicionais, acreditamos serem indispensáveis as seguintes informações:

- Responsável pelo tratamento dos seus Dados Pessoais;
- Princípios aplicáveis à proteção dos seus Dados Pessoais;
- Dados Pessoais, Tratamento de Dados Pessoais e Titular dos Dados;
- Categoria de Dados Pessoais que a IBC SECURITY trata na Aplicação;
- Finalidades para o tratamento dos seus Dados Pessoais;
- Fundamentos de Licitude;
- Prazo de conservação dos seus Dados Pessoais;
- Partilha dos seus Dados Pessoais;
- Transferências Internacionais de Dados Pessoais;
- Os seus direitos e como exercê-los;

- O Encarregado de Proteção de Dados;
- Segurança dos seus Dados Pessoais;
- Confidencialidade;
- Documentação Profissional Obrigatória;
- Folhas de Ponto e Gestão de Férias;
- Dados Biométricos;
- Notificações Push;
- Cessação do Contrato de Trabalho;
- Contactos;
- Alterações a esta Política de Proteção de Dados e de Privacidade.

---

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 execução do contrato de trabalho;
- 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 laboral, 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 identificação fiscal, o seu número de colaborador, 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. Dentro deste ciclo, entre outros, incluem-se o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, a limitação e o apagamento.

No contexto da Aplicação, o **Titular dos Dados** é o colaborador da IBC SECURITY que mantenha uma relação contratual laboral ativa com a empresa.

A Aplicação não se destina a menores de 18 anos e a **IBC SECURITY** não recolhe dados pessoais de menores através desta ferramenta.

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 pela IBC SECURITY (provenientes do contrato de trabalho)

Categoria de Dados Pessoais	Dados Pessoais
Dados de identificação pessoal	Nome completo, número de identificação fiscal (NIF)
Dados de identificação profissional	Número de colaborador, função, categoria profissional, data de admissão
Dados de contacto profissional	Endereço de email profissional
Dados das credenciais de segurança	Email e palavra-passe (encriptada)

4.2. Dados fornecidos diretamente pelo colaborador

Categoria de Dados Pessoais	Dados Pessoais
Dados de contactos de emergência	Nome, telefone(s) (primário e secundário) e notas de até 3 contactos de emergência designados pelo colaborador
Dados de documentação profissional	Imagens e ficheiros PDF dos documentos profissionais obrigatórios (Cartão profissional de segurança privada, Certificado SBVDAE/TAT/TAS, Cartão MAI) e respetivas datas de validade
Dados de folhas de ponto	Horas de entrada/saída, horas extraordinárias, observações mensais
Dados de pedidos de férias	Períodos solicitados, motivos, observações
Dados de confirmação de leitura	Marcas temporais de confirmação de leitura de comunicados e procedimentos internos

4.3. 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), identificador de dispositivo (para controlo de sessões concorrentes)
Dados de autenticação	Identificador de utilizador (UID), sessões de autenticação, data e hora do último login
Registos de auditoria	Eventos de login, submissão de folhas de ponto, upload de documentos, alterações de email ou

	palavra-passe, alterações de contactos de emergência

4.4. Dados biométricos

Categoria de Dados Pessoais	Dados Pessoais
Dados biométricos	Impressão digital ou reconhecimento facial — **processados exclusivamente no dispositivo, nunca transmitidos para servidores da IBC SECURITY ou terceiros** (ver secção 16)

Ressalvamos que a recolha dos dados pessoais constantes do ponto 4.1 é condição necessária para a execução do contrato de trabalho e para o cumprimento das obrigações legais da IBC SECURITY enquanto entidade empregadora no setor de segurança privada. A recolha dos dados constantes dos pontos 4.2 e 4.4 é facultativa, ficando sujeita à aceitação do colaborador, sem prejuízo das obrigações legais que imponham a apresentação de documentação profissional obrigatória.

5. Finalidades para o tratamento dos seus Dados Pessoais

O desenvolvimento e realização das várias atividades prosseguidas pela **IBC SECURITY** através da Aplicação significam a existência de um conjunto relevante de finalidades específicas, explícitas e legítimas para o tratamento dos seus Dados Pessoais:

Finalidades	Finalidades de Tratamento
Gestão da relação laboral	Autenticação e controlo de acesso à Aplicação, disponibilização de informação profissional ao colaborador
Processamento salarial	Disponibilização de recibos de vencimento e documentação fiscal associada
Gestão de escalas de trabalho	Publicação e consulta de escalas atribuídas ao colaborador
Comunicações internas	Divulgação de comunicados, procedimentos operacionais e instruções de serviço, incluindo confirmação de leitura
Gestão de férias	Receção, análise e aprovação de pedidos de férias; disponibilização de mapa de férias

Gestão de folhas de ponto	Receção e validação de folhas de ponto mensais submetidas pelo colaborador
Gestão documental	Upload, validação e controlo de validade de documentação profissional obrigatória nos termos da Lei n.º 34/2013
Gestão de contactos de emergência	Manutenção de contactos designados pelo colaborador para situações de emergência no local de trabalho
Notificações de serviço	Envio de notificações push relativas a novos recibos, novas escalas, comunicados, procedimentos e alertas de validade de documentos
Segurança da conta	Proteção contra acessos não autorizados através de palavra-passe forte, código por email, bloqueio biométrico 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
Execução do contrato (Art. 6.º, n.º 1, al. b) RGPD)	A **IBC SECURITY** trata os seus Dados Pessoais na medida em que os mesmos são necessários para a execução do contrato de trabalho.	Gestão da relação laboral, processamento salarial, gestão de escalas, comunicados e procedimentos internos, pedidos de férias, folhas de ponto
Cumprimento de obrigação jurídica (Art. 6.º, n.º 1, al. c) RGPD)	A **IBC SECURITY** trata os seus Dados Pessoais para cumprir obrigações legais a que está sujeita enquanto entidade empregadora e enquanto empresa de segurança privada.	Conservação de recibos de vencimento e documentação fiscal (10 anos); gestão de documentação profissional obrigatória nos termos da Lei n.º 34/2013; registos de auditoria
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	Segurança da conta (palavra-passe, biometria, bloqueio automático), registos de auditoria de acessos, controlo de sessões concorrentes

	ou direitos e liberdades fundamentais.	
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.	Receção de notificações push; designação de contactos de emergência; upload de imagens de documentação profissional

Contactos de emergência: Os contactos de emergência são dados pessoais de terceiros fornecidos pelo colaborador. O colaborador é responsável por informar as pessoas indicadas como contacto de emergência sobre esta designação e sobre o tratamento dos seus dados pelo empregador nos termos da presente Política.

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, ao abrigo das leis em vigor, 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, NIF, número de colaborador, email)	Durante a vigência do contrato de trabalho + 5 anos após cessação	Obrigações contratuais, Código do Trabalho
Recibos de vencimento e documentação fiscal	10 anos (Art. 40.º do Código Comercial, Art. 123.º do CIRC)	Obrigação legal
Escalas de trabalho	Durante a vigência do contrato + período legalmente exigido	Obrigação legal
Comunicados e procedimentos (e confirmações de leitura)	Até à data de validade definida pela IBC SECURITY ou eliminação automática	Interesse legítimo

Pedidos e mapa de férias	Durante a vigência do contrato + período legalmente exigido	Obrigação legal
Folhas de ponto	Até 1 ano após submissão (eliminação automática dos ficheiros antigos)	Necessidade operacional e interesse legítimo
Documentação profissional (cartão profissional, SBVDAE/TAT/TAS, MAI)	Pelo período exigido pela legislação de segurança privada (Lei n.º 34/2013) ou até cessação do contrato de trabalho	Obrigação legal
Contactos de emergência	Durante a vigência do contrato de trabalho	Execução do contrato
Tokens FCM (notificações)	Até logout, desinstalação da app ou invalidação automática	Necessidade técnica
Registos de login (login_events)	12 meses (eliminação mensal automática)	Interesse legítimo e RGPD
Registos de auditoria	Período definido pela legislação aplicável	Interesse legítimo e obrigação legal
Dados biométricos	Nunca armazenados pela IBC SECURITY (processamento local no dispositivo)	N/A

Durante o período de Tratamento dos seus Dados Pessoais, a **IBC SECURITY** garante que os mesmos são tratados em conformidade com esta Política de Proteção de Dados e de Privacidade. Assim que os seus Dados já não sejam necessários, a **IBC SECURITY** procederá à sua eliminação de forma segura e irreversível.

8. Partilha dos seus Dados Pessoais

Entidades com quem a IBC SECURITY partilha os seus Dados Pessoais	Porque partilhamos os seus Dados Pessoais
Recursos Humanos / Administração	Os seus dados (identificação, contactos, documentação profissional, folhas de ponto, pedidos de férias) são acedidos pela equipa de Recursos Humanos e Administração para gestão contratual, processamento salarial e cumprimento de obrigações legais.

Gerência	Os seus dados (escalas, pedidos de férias, comunicados dirigidos) são acedidos pela Gerência para gestão operacional da relação laboral.
Coordenação Técnica	Apenas os dados estritamente necessários (nome, número de colaborador, escalas e comunicados relevantes) são acedidos pela coordenação técnica para efeitos de organização operacional.
Contabilidade	Recibos de vencimento, folhas de ponto e documentação fiscal são partilhados para efeitos de processamento salarial e cumprimento de obrigações fiscais.
Autoridades competentes	Em cumprimento de obrigações legais, os Dados Pessoais poderão ser transmitidos a autoridades judiciais, administrativas (Autoridade para as Condições do Trabalho, Autoridade Tributária, PSP, GNR), de supervisão ou regulatórias.

Subcontratantes específicos:

Prestador	Serviço	Dados Processados	Localização	Garantias
Google LLC (Firebase)	Autenticação, base de dados (Firestore), armazenamento (Storage), notificações push (FCM), Cloud Functions	Todos os dados da conta, documentos carregados, tokens FCM	UE (europe-west1)	DPA Google Cloud, Cláusulas Contratuais-Tipo (SCCs), certificação ISO 27001
Google LLC (FCM)	Serviço de notificações push	Tokens de dispositivo, metadados de notificação	UE/EUA	DPA Google Cloud, EU-US Data Privacy Framework

A **IBC SECURITY não vende, aluga ou cede os seus Dados Pessoais a terceiros para fins comerciais ou de marketing.**

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 (nomeadamente, o serviço Firebase Cloud Messaging, utilizado para notificações push). Contudo, a **IBC SECURITY** apenas transfere os seus Dados Pessoais para fora do EEE:

- Quando a transferência for feita para uma localização ou através de um método ou em circunstâncias que a Comissão Europeia considere garantirem a proteção adequada dos seus Dados Pessoais;
- Quando tiver implementado cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia ou por uma autoridade de proteção de dados competente;
- Ao abrigo do EU-US Data Privacy Framework (quando aplicável); ou,
- Quando nenhuma das opções anteriores se aplicar, mas, ainda assim, a lei autorizar essa transferência.

Poderá solicitar informação detalhada sobre as medidas de segurança que a **IBC SECURITY** tem implementadas a respeito de transferências de Dados Pessoais para fora do EEE 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 é que a **IBC SECURITY** usa os seus Dados Pessoais e quais são os seus direitos. É por isso que a **IBC SECURITY** lhe disponibiliza todas estas informações nesta Política.
Direito de acesso (Art. 15.º)	Tem o direito de obter informação sobre que Dados Pessoais a **IBC SECURITY** trata e determinadas informações sobre a forma como esses Dados são tratados.
Direito de retificação (Art. 16.º)	Se os seus Dados estiverem incorretos ou incompletos, poderá pedir para a **IBC SECURITY** tomar medidas razoáveis para os corrigir.

Direito ao apagamento dos dados (Art. 17.º)	Permite-lhe solicitar o apagamento dos seus dados, desde que não existam fundamentos válidos para que a **IBC SECURITY** continue a usá-los (nomeadamente, obrigações legais laborais, fiscais ou do setor de segurança privada).
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 de retificação ou como alternativa ao apagamento.
Direito à portabilidade dos dados (Art. 20.º)	Tem o direito de obter e reutilizar determinados Dados Pessoais para os seus próprios fins. Aplica-se apenas aos Dados próprios que tenha fornecido à **IBC SECURITY** e que sejam tratados com base em consentimento ou execução de contrato, por meios automatizados.
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, nomeadamente ao tratamento baseado em interesses legítimos.
Direito de apresentar queixa	Tem o direito de apresentar queixa junto da autoridade de controlo competente, a **Comissão Nacional de Proteção de Dados – CNPD** (www.cnpd.pt, Av. D. Carlos I, 134, 1.º, 1200-651 Lisboa, +351 213 928 400, geral@cnpd.pt).
Direito de revogação do consentimento	Tem o direito de retirar o consentimento a qualquer momento, sem comprometer a licitude do tratamento efetuado anteriormente. Aplica-se ao tratamento de dados cuja base legal seja o consentimento (notificações push, contactos de emergência, upload de documentos).

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
- **Entrega presencial:** Nos serviços de Recursos Humanos na sede da IBC Security.

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, mediante comunicação ao

titular. Para efeitos de verificação de identidade, poderá ser solicitada documentação adicional antes do processamento do pedido.

Tendo em conta a relação laboral existente, determinados direitos (nomeadamente o direito ao apagamento) poderão ser limitados pela necessidade de cumprimento de obrigações legais do empregador, designadamente em matéria fiscal, laboral e de segurança privada.

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 seio da **IBC SECURITY** 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 constantes das leis de proteção de dados vigente e conexa à matéria de proteção de dados pessoais;
2. Prestar aconselhamento à **IBC SECURITY**;
3. Cooperar com as Autoridades de Controlo dos respetivos Estados-Membros da União Europeia (em Portugal a CNPD — Comissão Nacional de Proteção de Dados); e,
4. Constituir um ponto de contacto com as Autoridades de Controlo e com os respetivos titulares de dados sobre quaisquer questões relacionadas com matérias de proteção de dados.

Poderá a qualquer momento, por escrito, contactar o encarregado de proteção de dados da **IBC SECURITY** para quaisquer questões relacionadas com a proteção de dados e a sua privacidade através do email **dpo@rgpdconsultores.pt**.

12. Segurança dos seus Dados Pessoais

Os seus Dados Pessoais serão tratados pela **IBC SECURITY**, no contexto das finalidades identificadas na presente Política, com recurso a medidas técnicas e organizativas adequadas para promover a respetiva segurança e integridade.

12.1. Medidas técnicas específicas da Aplicação

- **Encriptação em trânsito:** Todas as comunicações entre a Aplicação e os servidores utilizam protocolo TLS (Transport Layer Security);
- **Encriptação em repouso:** Os dados armazenados no Firebase Firestore e Firebase Storage são encriptados em repouso;

- **Autenticação segura:** Autenticação via Firebase Authentication com política de palavra-passe forte (mínimo 12 caracteres, incluindo maiúsculas, minúsculas, números e símbolos);
- **Bloqueio de ecrã automático:** Bloqueio automático da sessão quando a Aplicação entra em segundo plano, com reautenticação biométrica ou logout completo;
- **Código por email para operações sensíveis:** Operações críticas (alteração de email, alteração de palavra-passe, gestão de contactos de emergência, acesso a recibos de vencimento) exigem verificação por código de 6 dígitos enviado para o email do colaborador;
- **Armazenamento seguro de credenciais:** Dados sensíveis locais armazenados em Keychain (iOS) / Keystore (Android);
- **Regras de acesso granulares:** Regras de segurança que garantem que cada colaborador acede exclusivamente aos seus próprios dados, com exceção dos dados partilhados pela função exercida (escalas, comunicados, procedimentos, mapa de férias);
- **Deteção de instalação nova:** Sessões anteriores são invalidadas em novos dispositivos para prevenir acessos não autorizados;
- **Controlo de sessões concorrentes:** Apenas uma sessão ativa por conta em simultâneo.

12.2. Medidas organizativas

- **Princípio do privilégio mínimo:** Cada operador administrativo acede apenas aos dados estritamente necessários para as suas funções;
- **Perfis de acesso diferenciados:** O sistema aplica perfis de acesso distintos (admin_full, admin_staff, gerencia_full, admin_temp, employee, employee_office, employee_tech, tech_admin) que limitam a visibilidade e edição de dados conforme a função;
- **Registo de acessos:** Todas as ações de consulta e modificação de dados de colaboradores são registadas em log de auditoria;
- **Formação:** Os administradores e operadores recebem formação sobre proteção de dados e sigilo profissional;
- **Sigilo profissional:** Todos os colaboradores da **IBC SECURITY** estão vinculados ao dever de sigilo profissional nos termos da Lei n.º 34/2013;
- **Cópias de segurança:** Backups diários automáticos da base de dados (retenção de 14 dias) e backups periódicos do armazenamento (cada 5 dias), armazenados na UE;
- **Gestão de incidentes:** Procedimento interno de resposta a violações de dados, incluindo notificação à CNPD no prazo de 72 horas quando aplicável.

Contudo, dado que a transmissão de informação pela Internet não é completamente segura, a **IBC SECURITY** não pode garantir a segurança dos seus Dados quando transmitidos em rede aberta.

13. Confidencialidade

A **IBC SECURITY** reconhece que a informação laboral e profissional que consta da Aplicação é confidencial e sensível. A **IBC SECURITY** não vende, aluga, distribui, nem disponibiliza comercialmente ou de outra forma os Dados Pessoais dos seus colaboradores a nenhuma entidade terceira, exceto nos casos em que necessita partilhar informação com os Prestadores de Serviço identificados na secção 8, ou quando exista obrigação legal de o fazer.

---

14. Documentação Profissional Obrigatória

14.1. Documentação exigida por lei

Nos termos da Lei n.º 34/2013 (regime da atividade de segurança privada) e legislação conexa, a **IBC SECURITY** tem o dever legal de manter atualizada e disponível a seguinte documentação relativa aos seus colaboradores vigilantes:

- **Cartão profissional de segurança privada (MAI)** — emitido pela Polícia de Segurança Pública;
- **Certificado de formação profissional** (SBVDAE, TAT ou TAS, conforme função);
- **Registo criminal** — cuja validade é acompanhada por alertas de expiração (sem upload do próprio certificado, que é conservado em suporte físico na sede).

14.2. Upload e gestão

O colaborador pode submeter através da Aplicação imagens ou ficheiros PDF dos documentos acima referidos, bem como atualizar as respetivas datas de validade. Os documentos carregados ficam armazenados no Firebase Storage com regras de acesso que limitam a sua consulta ao próprio colaborador, aos Recursos Humanos e à Gerência.

14.3. Alertas de validade

A Aplicação envia notificações push automáticas com 90, 60 e 30 dias de antecedência em relação à data de expiração de cada documento profissional, de forma a permitir ao colaborador a sua renovação atempada.

---

15. Folhas de Ponto e Gestão de Férias

15.1. Folhas de ponto

A partir do dia 20 de cada mês, a Aplicação permite ao colaborador submeter a folha de ponto do mês em curso, indicando horas efetivamente trabalhadas. As folhas de ponto submetidas são validadas pelos serviços administrativos e conservadas por 1 ano antes de eliminação automática.

15.2. Pedidos de férias

O colaborador pode submeter pedidos de férias através da Aplicação, indicando o período pretendido. Os pedidos são encaminhados para aprovação da Gerência e, uma vez decididos, o colaborador recebe notificação push com o resultado (aprovação ou rejeição). O mapa de férias consolidado é disponibilizado a todos os colaboradores autorizados para consulta.

---

16. Dados Biométricos

A Aplicação oferece a possibilidade de autenticação biométrica (impressão digital ou reconhecimento facial) para desbloqueio da sessão. Estes dados biométricos são:

- **Processados exclusivamente no dispositivo** do colaborador, através dos mecanismos nativos do sistema operativo (Android BiometricManager / iOS Face ID ou Touch ID);
- **Nunca transmitidos** para servidores da **IBC SECURITY**, Firebase ou quaisquer terceiros;
- **Nunca armazenados** pela Aplicação — apenas o resultado da verificação (sucesso/falha) é utilizado para desbloqueio local.

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

A utilização da biometria é facultativa — o colaborador pode optar pela autenticação exclusivamente por palavra-passe.

---

17. Notificações Push

A Aplicação utiliza o serviço Firebase Cloud Messaging (FCM) para envio de notificações push relativas a:

- Disponibilização de novos recibos de vencimento;
- Publicação de novas escalas de trabalho;
- Novos comunicados e procedimentos internos;
- Alertas de expiração de documentos profissionais (90, 60 e 30 dias antes da data de validade);
- Aprovação ou rejeição de pedidos de férias;
- Lembretes de submissão de folha de ponto;
- Outras comunicações operacionais relevantes.

As notificações push podem ser **desativadas a qualquer momento** através das definições do dispositivo (Android: Definições → Aplicações → IBC Security → Notificações; iOS: Definições → Notificações → IBC Security). A desativação não impede o funcionamento da Aplicação, mas o colaborador poderá não ser informado atempadamente de comunicações relevantes.

---

18. Cessação do Contrato de Trabalho

Em caso de cessação do contrato de trabalho (por qualquer motivo), a **IBC SECURITY** procederá a:

- **Bloqueio imediato do acesso à Aplicação** — A conta é desativada na data de cessação efetiva do contrato;
- **Revogação de tokens de notificação** — Os tokens FCM são invalidados;
- **Eliminação de documentos do dispositivo** — Os dados cacheados no dispositivo deixam de ser acessíveis;
- **Conservação de dados em servidor** — Os Dados Pessoais são conservados em servidor pelos períodos legalmente exigidos (ver secção 7), designadamente para efeitos de obrigações fiscais, laborais e de segurança privada;
- **Eliminação dos dados após expiração do prazo legal** — Findo o prazo de conservação aplicável, os Dados são eliminados de forma segura e irreversível.

O ex-colaborador mantém o direito de exercer os seus direitos de titular dos dados (acesso, retificação, apagamento, etc.) após a cessação do contrato, nos termos da secção 10.

---

19. Contactos

Caso tenha alguma questão ou pretenda obter mais informações acerca de como tratamos os seus Dados Pessoais ou sobre as nossas práticas em matéria de segurança da informação, por favor, não hesite em contactar-nos através dos seguintes endereços de contacto:

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 Email geral: info@ibcsecurity.com Telefone: +351 289 093 344

---

20. Alterações a esta Política de Proteção de Dados e de Privacidade

A **IBC SECURITY** poderá atualizar periodicamente a presente Política de Proteção de Dados e Privacidade. Ao efetuar alterações à presente Política, será adicionada uma nova data no início da mesma.

Quaisquer alterações significativas serão comunicadas ao colaborador através de:

- Notificação na Aplicação e solicitação de nova aceitação, quando aplicável;
- Comunicação por email para o endereço registado na conta.

A utilização continuada da Aplicação após a comunicação de alterações constitui aceitação da Política atualizada. O colaborador pode, a qualquer momento, consultar a versão mais recente desta Política nas definições da Aplicação ou solicitá-la aos serviços de Recursos Humanos.

---

21. Legislação Aplicável

A presente Política de Proteção de Dados e de Privacidade rege-se pela seguinte legislação:

- **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 7/2009, de 12 de fevereiro** — Código do Trabalho;
- **Lei n.º 34/2013, de 16 de maio** (com alterações pela Lei n.º 46/2019) — Regime do exercício da atividade de segurança privada;
- **Portaria n.º 273/2013, de 20 de agosto** — Regulamentação da Lei n.º 34/2013.

A presente Política de Proteção de Dados e de Privacidade foi redigida em conformidade com o Regulamento (UE) 2016/679 (RGPD), a Lei n.º 58/2019 e as orientações da Comissão Nacional de Proteção de Dados (CNPD).