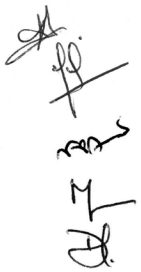
FUNDAÇÃO CEBI

REGULAMENTO INTERNO PROTEÇÃO DE DADOS PESSOAIS



INTRODUÇÃO

A CEBI – Fundação para o Desenvolvimento Comunitário de Alverca, doravante designada por Fundação CEBI, é uma Instituição Particular de Solidariedade Social, sem fins lucrativos, que dirige a sua atividade para crianças, jovens, idosos e famílias, com particular atenção aos mais desfavorecidos.

Com sede na Rua Maria Eduarda Segura de Faria, 2, em Alverca do Ribatejo, a sua atividade abrange as seguintes áreas de intervenção:

Educação: com oferta educativa desde o berçário até ao ensino secundário.

Social:

- Emergência Social - Acolhimento Temporário de crianças em risco e de famílias em Comunidade de Inserção;
- Intervenção Social e Comunitária - Apoio Social e Psicológico à comunidade;
- Apoio a Idosos - ERPI, Centro de Dia e Apoio Domiciliário.

Saúde: Clínica de Medicina Física e Reabilitação

A sua intervenção estende-se para além da cidade de Alverca com um equipamento social no concelho de Mafra, designado Apoio Comunitário Integrado.

A Fundação CEBI rege-se pela Lei-quadro das Fundações e pelo Estatuto das IPSS's.

O Regulamento Geral da Proteção de Dados (RGPD), aprovado com o n.º 679/2016 pelo Parlamento Europeu e pelo Conselho da União Europeia, em 27 de abril de 2016 e publicado em 4 de maio desse ano.

Com vista a regulamentar a sua implementação na Fundação CEBI, é emitido o presente regulamento, que enquadra as obrigações dispostas no RGPD quanto à proteção de dados pessoais.

CAPÍTULO I
DISPOSIÇÕES GERAIS

ARTIGO 1.º
OBJETIVO

1. O presente Regulamento estabelece as regras a observar pelos serviços da Fundação CEBI, no que diz respeito ao tratamento de dados pessoais e à circulação desses dados, visando integrar no quadro regulamentar interno os princípios e normas que regulam na ordem jurídica a matéria relativa à reserva e confidencialidade de dados pessoais.

ARTIGO 2.º
ÂMBITO E CAMPO DE APLICAÇÃO

1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios automatizados e não automatizados, independentemente da fonte e da natureza do respetivo suporte.

2. No âmbito das suas diversas atividades, e no que respeita, nomeadamente, aos dados das pessoas singulares, a Fundação CEBI e, consequentemente, todos os seus colaboradores, devem cumprir, as disposições deste regulamento, bem como demais legislação em vigor, sobre esta matéria.

3. Consideram-se colaboradores, para efeitos deste Regulamento, os que tenham com a Fundação uma relação, seja de trabalho, ou de qualquer outra natureza, do local de trabalho e da função que desempenham, incluindo-se:
   - Membros dos órgãos sociais;
   - Trabalhadores, independentemente do tipo de vínculo;
   - Prestadores de serviços;
   - Voluntários;
   - Estagiários;
   - Contratados no regime de emprego inserção
   - Fornecedores.

4. Todos os colaboradores que tratem/utilizem dados pessoais são individualmente responsáveis pelo cumprimento das disposições legais e regulamentares aplicáveis, bem como têm a obrigação de garantir a confidencialidade dos dados como parte indissociável das suas funções, mesmo após o termo das suas funções, pelo período a que estão legalmente obrigados.

5. Este regulamento interno vincula toda a estrutura organizacional da Fundação, cuja atividade envolva a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição de dados pessoais e deve permitir à Fundação realizar os seus processos de forma eficaz e manter ou melhorar a sua imagem positiva nas comunidades em que atua.

ARTIGO 3.º
REGRAS GERAIS

1. As responsabilidades da Fundação CEBI na proteção de dados pessoais, são cometidas pelo presente Regulamento aos respetivos Diretores (DIR) e Responsáveis de Área (RAR), e a todos os Colaboradores designados por estes para o tratamento de dados pessoais, a partir daqui designados como responsáveis. As decisões dos DIR e RAR de atribuírem competências aos responsáveis devem ser previamente articuladas com o Encarregado de Proteção de Dados (EDP) e comunicadas à Coordenação Geral no prazo de 24 horas.

2. Os DIR e RAR deverão tomar a iniciativa de elaborar os procedimentos necessários ao tratamento dos dados tratados no âmbito do seu Departamento ou área de responsabilidade e ao cumprimento deste regulamento, solicitando, se necessário, o apoio do Encarregado de Proteção de Dados (EPD).

3. O presente regulamento transcreve e adapta as regras gerais do RGPD, aprovado pelo Parlamento Europeu, o que não dispensa os responsáveis pelo tratamento de dados pessoais de conhecerem as regras específicas estabelecidas por aquele Regulamento, aplicáveis a cada uma das situações observadas pelos serviços da Fundação.

4. O não cumprimento das obrigações pode ter consequências disciplinares e outras que legalmente possam estar previstas.

5. Todas as falhas e violações, no âmbito deste regulamento devem ser reportadas ao EPD no prazo de 24 horas após a sua verificação ou tomada de conhecimento.

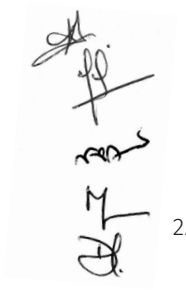
ARTIGO 4.º
ENCARREGADO DE PROTEÇÃO DE DADOS

1. De acordo com o disposto no art.º 37.º do RGPD, é criada a função de Encarregado de Proteção de Dados (EPD), que reporta à Coordenação Geral.

2. São atribuições do encarregado de proteção de dados:
   a. Promover o conhecimento junto dos DIR, RAR e responsáveis do conteúdo do RGPD na parte a cada um aplicável, aconselhando-os e supervisionando o cumprimento deste regulamento e da demais legislação aplicável;
   b. Informar e aconselhar os colaboradores quanto às disposições regulamentares em matéria de proteção de dados;
   c. Controlar a conformidade com o RGPD;
   d. Prestar aconselhamento, quando tal for solicitado, relativamente à Avaliação do Impacto na Proteção de Dados (AIPD) (Art.º 35.º do RGPD);
   e. Cooperar com a autoridade de controlo;
   f. Ser o ponto de contacto para a autoridade de controlo sobre questões de tratamento, incluindo consulta prévia (Art.º 36.º do RGPD).

ARTIGO 5.º
DEFINIÇÕES

1. Dados Pessoais – "Informação relativa a uma pessoa singular identificada ou identificável (Titular dos Dados)"; de qualquer tipo ou natureza ou forma de armazenamento, em poder da Fundação, incluindo, designadamente: nome, idade, data de nascimento, morada, género, dados sobre documentos pessoais, estado civil, número de filhos, religião, filiação sindical, bem como todos dados que possam ser usados direta ou indiretamente para identificar uma pessoa.



2. Tratamento – "Uma operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição".

3. Responsável pelo tratamento – A Fundação CEBI enquanto organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios de tratamento de dados pessoais.

4. Subcontratante – "Pessoa singular ou coletiva que trate os dados pessoais por conta e em nome do responsável pelo tratamento destes".

5. Consentimento – "manifestação de vontade do titular dos dados prestada, livre e especificamente, pela qual aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais, que lhe dizem respeito, sejam objeto de tratamento".

6. Violação de dados pessoais – "Uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

CAPÍTULO II
PRINCÍPIOS E RESPONSABILIDADES DE PROTEÇÃO DE DADOS

ARTIGO 6.º
PRINCÍPIOS

1. São os seguintes os princípios relativos ao tratamento e recolha de dados pessoais:
   a. "Licitude, lealdade e transparência" - Os responsáveis tratam os dados pessoais de forma lícita, leal e transparente, obtendo dos titulares dos dados o consentimento necessário para o respetivo tratamento.
   b. "Limitação das finalidades"- Os dados pessoais são recolhidos para uma determinada finalidade, explícita e legítima, limitados à informação necessária para o seu processo, não podendo incidir, a não ser com o consentimento prévio do titular dos dados, sobre dados pessoais referentes a convicções religiosas, filosóficas ou políticas, filiação partidária e sindical, vida privada, origem racial ou étnica, saúde ou vida sexual ou orientação sexual, bem como o tratamento de dados genéticos e biométricos.
   c. "Minimização dos dados" - Os dados recolhidos são adequados, pertinentes e limitados ao que é necessário para a finalidade do tratamento.
   d. "Exatidão" - Devem ser tomadas as medidas adequadas para que os dados sejam exatos e atualizados sempre que necessário, devendo os inexatos, tendo em conta a finalidade de tratamento, serem retificados ou apagados sem demora.
   e. "Limitação da Conservação" - Os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares apenas durante o período necessário para a finalidade do respetivo tratamento.
   f. "Integridade e Confidencialidade" - Devem ser adotadas medidas para que os dados sejam tratados com segurança, incluindo a proteção contra o acesso e tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

ARTIGO 7.º
RESPONSABILIDADES

1. Os responsáveis, incluindo o Departamento de Sistemas de Informação (DSI) da Fundação, relativamente ao tratamento informatizado, devem observar o cumprimento dos princípios definidos no artigo anterior, efe-

tuando registos que o possam comprovar a qualquer momento, devendo, designadamente:

a. Garantir a operacionalidade e fiabilidade dos suportes de dados:
   i. Considerando a disponibilidade de dados;
   ii. Zelando pela qualidade e fiabilidade dos dados, nomeadamente pela persistência dos dados informatizados em caso de falha;
   iii. Assegurando a segurança de transmissão de dados em serviços prestados por terceiros, para utentes da Fundação, a destinatários externos ou subcontratantes.

b. Controlar acesso a dados por utilizadores e:
   i. Contribuir para definição de políticas de segurança e controlo no acesso a dados, de acordo com procedimentos internos da Fundação;
   ii. Implementar e manter políticas de segurança, conforme definidas na alínea anterior;
   iii. Zelar pelo cumprimento de regulamento, normas e boas-práticas aplicáveis ao manuseamento de dados, incluindo, mas não se limitando a aplicação de normas técnicas de segurança ativa e passiva de acesso aos dados;
   iv. Dotar os sistemas de informação de soluções que permitam rastrear e identificar todos os acessos a dados pessoais por parte de utilizadores.

c. Colaborar com EPD:
   i. Na Avaliação do Impacto na Proteção de Dados (AIPD);
   ii. No controlo e auditorias ao RGPD;
   iii. Na eventualidade de falhas ou violações do presente regulamento.

d. Elaborar os procedimentos necessários ao tratamento dos dados no âmbito do seu Departamento ou área de responsabilidade e ao cumprimento deste regulamento;

e. Contribuir para a prevenção e mitigação de riscos:
   i. Alertando o EPD, ou outras entidades da Fundação, para situações de risco ou de incumprimento do presente regulamento interno ou do RGPD em geral;
   ii. Colaborando na validação de novas ferramentas de tratamento de dados a instalar na Fundação.

2. O DSI deve promover a formação de responsáveis no manuseamento de dados informatizados no âmbito do RGPD, sendo corresponsável com os outros departamentos no cumprimento do número anterior sempre que estejam envolvidos dados informatizados.

ARTIGO 8.º
LICITUDE DO TRATAMENTO

1. O tratamento de dados pessoais só é lícito quando se verifique pelo menos uma das seguintes situações:
   a. Decorra da lei;
   b. O Titular tenha dado o seu consentimento para o tratamento;
   c. O tratamento é necessário para a execução de contrato ou para diligências pré-contratuais;
   d. O tratamento é necessário para cumprimento de obrigação jurídica;
   e. O tratamento é necessário para a defesa de interesses vitais do Titular;
   f. O tratamento é necessário ao exercício de funções de interesse público;
   g. O tratamento é necessário para efeito dos interesses do responsável pelo tratamento exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do Titular, que exijam a proteção dos dados, em especial se o titular for criança.

2. Os dados pessoais são recolhidos pelos responsáveis pelo tratamento de acordo com os princípios e com a licitude requerida.

3. Qualquer alteração ao método de recolha e ao tratamento de dados pessoais deverá ser previamente comunicada ao EPD para verificar a sua viabilidade e conformidade com os requisitos legais.

ARTIGO 9.º
CONSENTIMENTO

1. Quando o tratamento de dados for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu expressamente o seu consentimento para o tratamento dos seus dados pessoais.

2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita, que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples.

3. Quando for necessário o consentimento do titular para o tratamento dos dados pessoais de crianças, é lícito se elas tiverem pelo menos 16 anos e quando o próprio tenha dado consentimento. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança que, para o efeito, terão que apresentar documento idóneo que lhe confira o exercício do poder parental.

4. O titular dos dados tem direito a retirar o seu consentimento em qualquer momento, sem comprometer a licitude do tratamento, efetuado com base no consentimento anterior.

5. O consentimento deve ser igualmente fácil de retirar como de dar.

ARTIGO 10.º
CATEGORIAS ESPECIAIS DE DADOS

1. Por norma "é proibido o tratamento de dados pessoais, que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa".

2. O disposto no número anterior admite as seguintes exceções:
   a. Se o titular dos dados tiver dado o seu consentimento explicito para uma ou mais finalidades específicas, exceto se o direito nacional previr que a proibição não pode ser anulada pelo titular dos dados.
   b. Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e proteção social.
   c. Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito ou por força de um contrato com um profissional de saúde, sob reserva de serem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade, nos termos do direito nacional ou da União Europeia.
   d. Outras situações em que a proibição não se aplica nos termos do art.º 9º do RGPD.

CAPÍTULO III
DIREITOS DO TITULAR DOS DADOS

ARTIGO 11.º
DADOS RECOLHIDOS JUNTO DO TITULAR

1. Os DIR e RAR tomam as medidas adequadas para que possam ser fornecidas ao Titular as seguintes informações:
   a. A identidade e os contactos do responsável pelo tratamento;
   b. Os contactos do EPD;
   c. As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
   d. Os interesses legítimos do responsável pelo tratamento ou de terceiro, se o tratamento se basear na alínea f), do n.º 1, do art.º 8.º deste regulamento.
   e. Os destinatários ou categoria de destinatários dos dados pessoais, se os houver.

2. Para além das informações acima referidas, os responsáveis devem prestar ao titular as seguintes informações adicionais:
   a. Prazo de conservação dos dados pessoais;
   b. O direito de acesso aos seus dados pessoais, bem como à sua retificação ou ao seu apagamento, bem como o direito de se opor ao tratamento e o direito à portabilidade dos dados;
   c. O direito de retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento, efetuado com base no consentimento dado anteriormente;
   d. O direito de apresentar reclamação a uma entidade de controlo;
   e. Se a comunicação de dados constitui ou não uma obrigação legal ou contratual e se o titular está obrigado a fornecer os dados e as eventuais consequências de as não apresentar.

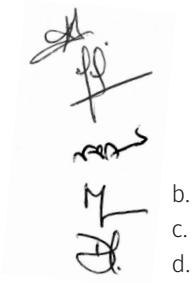
ARTIGO 12.º
DADOS NÃO RECOLHIDOS JUNTO DO TITULAR

1. Quando os dados pessoais não forem recolhidos junto do titular, os responsáveis devem comunicar-lhe as informações referidas no art.º 11.º:
   a. Num prazo razoável após a obtenção dos dados, o mais tardar dentro de um mês;
   b. Se os dados pessoais se destinam a ser utilizados para fins de comunicação com o titular, o mais tardar no momento da primeira comunicação;
   c. Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação.

2. Quando os DIR ou RAR pretenderem utilizar os dados pessoais para outra finalidade, que não seja aquela para o qual os dados foram obtidos, fornecem ao titular as informações sobre esse fim e as informações pertinentes do art.º 11.º que justificam a utilização.

ARTIGO 13.º
OUTROS DIREITOS DO TITULAR DOS DADOS

1. Os DIR ou RAR, no que se refere aos dados da sua responsabilidade, fornecem ao respetivo titular, no âmbito dos seus direitos inscritos no RGPD e quando o solicite, o direito de aceder aos seus dados pessoais e às seguintes informações:
   a. Direito de acesso a informação ligada ao tratamento dos seus dados pessoais e outros direitos já referidos no art.º 11.º;



b. Direito à retificação dos dados;
c. Direito ao apagamento dos dados (“direito de ser esquecido”);
d. Direito à limitação do tratamento;
e. Direito à portabilidade dos dados;
f. Direito de oposição.

ARTIGO 14.º
OBRIGAÇÃO DE NOTIFICAÇÃO

1. Os DIR ou RAR, responsáveis pelo tratamento, comunicam a cada destinatário a quem os dados pessoais tenham sido transmitidos, qualquer retificação ou apagamento, ou limitação do tratamento.

CAPÍTULO IV
GARANTIA E SEGURANÇA NO TRATAMENTO DE DADOS

ARTIGO 15.º
OBRIGAÇÕES GERAIS

1. Os responsáveis aplicam as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com este regulamento e que as mesmas são revistas e atualizadas de acordo com as necessidades.

ARTIGO 16.º
PROTEÇÃO DE DADOS DESDE A CONCEÇÃO E POR DEFEITO

1. Os responsáveis aplicam, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, para assegurar a eficácia dos princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento de forma a garantir a proteção dos direitos dos titulares. Igualmente é assegurado que, por defeito, só sejam tratados os dados necessários à finalidade específica do tratamento.

ARTIGO 17.º
REGISTO DAS ATIVIDADES DE TRATAMENTO

1. Cada responsável atualiza e conserva um registo de todas as atividades de tratamento sob a sua responsabilidade, que deve ser remetido ao EPD, onde conste:
   a. O nome e os contactos do responsável pelo tratamento e do EPD;
   b. A finalidade do tratamento;
   c. A descrição das categorias de titulares de dados e das categorias de dados;
   d. As categorias de destinatários a quem os dados foram ou serão divulgados;
   e. Descrição das medidas técnicas e organizativas, no domínio da segurança.

ARTIGO 18.º
SUBCONTRATANTE

1. Quando o tratamento de dados for efetuado por outrem, por conta da Fundação, os responsáveis recorrem apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas à satisfação dos requisitos do RGPD e assegure os direitos dos titulares de dados.

2. Este tratamento deve ser regulado por contrato, que vincule o subcontratante ao responsável pelo tratamento e contemple as disposições do artigo 28.º daquele regulamento.

ARTIGO 19.º
SEGURANÇA DO TRATAMENTO DE DADOS PESSOAIS

1. As DIR ou RAR aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, tais como:
   a. A pseudonimização e a cifragem dos dados pessoais;
   b. A capacidade de assegurar a confidencialidade, integridade, disponibilidade dos sistemas e dos serviços de tratamento;
   c. A guarda de dados pessoais em suporte físico em local devidamente fechado e de acesso restrito apenas a pessoas autorizadas;
   d. A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais, de forma atempada, no caso de um incidente físico ou técnico;
   e. Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

2. Em caso de violação de dados pessoais, o responsável pelo tratamento, comunica os factos ao EPD até 3 horas após a sua verificação, para que este as notifique à autoridade de controlo (CNPD) até 72 horas após o conhecimento da situação.

3. Quando a violação de dados for suscetível de implicar um risco elevado para os direitos do Titular dos dados, o EPD comunica igualmente a ocorrência ao Titular dos dados.

ARTIGO 20.º
AVALIAÇÃO DO IMPACTO SOBRE A PROTEÇÃO DE DADOS (AIPD)

1. Quando um tratamento de dados utiliza novas tecnologias e for suscetível de implicar grande risco para os direitos dos seus titulares, o responsável pelo tratamento procede, antes de o iniciar, a uma avaliação do impacto (AIPD), para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco.

2. A avaliação do impacto (AIPD), caso se venha a efetivar, deve seguir as orientações do art.º 35.º do RGPD.

3. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco, que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais.

Alverca do Ribatejo, 17 de Abril de 2018

O Conselho de Administração

REGULAMENTO INTERNO
PROTEÇÃO DE DADOS PESSOAIS

WWW.FCEBI.ORG