POLÍTICA DE PROTEÇÃO E SEGURANÇA DE DADOS PESSOAIS

DECLARAÇÃO E OBJETIVO DESTA POLÍTICA

1. **GALEAZZI & ASSOCIADOS CONSULTORIA E SERVIÇOS DE GESTÃO EMPRESARIAL LTDA** (doravante "a Empresa") compromete-se a garantir que todos os dados pessoais tratados pela Empresa sejam tratados de acordo com os padrões legais de proteção e segurança de dados pessoais exigidos pelas Leis de Proteção de Dados.

2. Confirmamos, para os fins da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais ("LGPD"), que a Empresa é uma controladora de dados pessoais de seus funcionários que possuem conexão com a relação de trabalho. Isso significa que compete à empresa as decisões referentes ao tratamento destes dados pessoais, bem como os propósitos para os quais estes dados pessoais são tratados.

3. Os objetivos desta política de proteção e segurança de dados pessoais são:

    a. informar nossos funcionários e colaboradores sobre quais dados pessoais dos funcionários, clientes, fornecedores, e demais terceiros (em conjunto, "titulares dos dados pessoais" que poderão ser coletados e tratados e o que a Empresa faz com esses dados pessoais;
    b. definir as regras de proteção de dados e as hipóteses legais de tratamento que devem ser satisfeitas quando a Empresa trata (isto é, coleta, recebe, manipula, processa, transfere e armazena, entre outras operações) dados pessoais e garantir que os funcionários entendam estas regras e os padrões legais; e
    c. esclarecer os direitos, responsabilidades e deveres dos funcionários em relação à proteção e segurança dos dados pessoais.

4. Esta política pode ser alterada a qualquer momento, a livre critério da Empresa.

5. Os termos usados nesta política tem sua definição igual àquela da LGPD.

PRINCÍPIOS DE PROTEÇÃO DE DADOS

6. Os funcionários cujo trabalho envolve lidar com dados pessoais de outros funcionários ou outras pessoas devem cumprir esta política e os seguintes princípios de proteção de dados:
    a. Dados pessoais devem ser tratados de forma legal, justa e transparente. A Empresa sempre deve ter uma hipótese legal de tratamento, conforme previsto no artigo 7º da LGPD, para realizar qualquer operação de tratamento de dados pessoais. Por exemplo, os dados pessoais podem ser tratados conforme necessário para executar um contrato (incluindo o contrato de emprego), para cumprir uma obrigação legal à qual a Empresa esteja sujeita, ou mesmo pelo interesse legítimo da Empresa. O titular dos dados deve ser informado que a Empresa controla suas informações, sobre quais são os objetivos do tratamento de dados pessoais realizado pela Empresa, e com quem tais dados podem ser compartilhados.
    b. Dados pessoais podem ser tratados apenas para propósitos legítimos, específicos, explícitos e informados ao titular de dados, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Os dados pessoais não podem ser coletados para uma finalidade e usados para outra. Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o propósito original, a Empresa deverá informar previamente o titular sobre tais mudanças.
    c. O tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, e deve se limitar ao mínimo necessário para a realização de suas finalidades. A Empresa coleta dados pessoais apenas na medida do necessário para a finalidade específica notificada ao titular dos dados.
    d. A Empresa deve realizar todos os esforços razoáveis para garantir que informações imprecisas, inexatas ou desatualizadas sejam retificadas ou excluídas sem demora. Dados pessoais serão verificados quando coletados e verificações regulares serão feitas posteriormente.
    e. Dados pessoais são mantidos apenas pelo período necessário para seu tratamento de acordo com sua finalidade. A Empresa adota todas as medidas razoáveis para excluir os dados quando deixarem de ser necessários ou pertinentes ao alcance da finalidade específica almejada.
    f. A empresa adota medidas de segurança, técnicas e administrativas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

RESPONSABILIDADE PELA PROTEÇÃO E SEGURANÇA DOS DADOS

7. **Manter padrões adequados de proteção e segurança de dados pessoais é tarefa de todos os funcionários**. Esta política e as regras nela contidas se aplicam a todos os funcionários, independentemente de cargo, senioridade e função. Todo os funcionários têm responsabilidade pessoal para tratar dados pessoais somente de acordo com os princípios e regras estabelecidos nesta política e garantir que sejam tomadas medidas adequadas para proteger a segurança dos dados. Gerentes e outros funcionários em posição de

liderança têm responsabilidade especial de educar pelo exemplo e monitorar e reforçar a conformidade com esta política.

8. Qualquer violação desta política será considerada grave e poderá resultar em ações disciplinares, incluindo demissão. Violações significativas ou deliberadas, como o acesso a dados pessoais de funcionários ou terceiros sem autorização ou razão legítima para tal podem constituir conduta grave e podem levar à demissão por justa causa.

9. Perguntas relacionadas a esta política ou solicitações de informações adicionais devem ser direcionadas para o Encarregado de Proteção de Dados ("EPD") da Empresa. O EPD deve ser notificado se esta política for violada ou se houver suspeita de violação.

DADOS PESSOAIS ABRANGIDOS POR ESTA POLÍTICA

10. Esta política abrange dados pessoais de pessoa natural (física) identificada ou identificável, relacionados a funcionários presentes, passados ou futuros da Empresa ou a qualquer outro indivíduo cujos dados pessoais sejam controlados e tratados pela Empresa, e/ou que tenha sido obtido, recebido, armazenado, organizado, divulgado, transferido, alterado, recuperado, usado, processado, transportado ou destruído pela Empresa.

11. Esses dados pessoais estão sujeitos às salvaguardas legais estabelecidas nas Leis de Proteção de Dados, incluindo (mas não se limitando) a LGPD.

DADOS PESSOAIS DOS FUNCIONÁRIOS COLETADOS PELA EMPRESA

12. A Empresa coleta os seguintes dados pessoais de seus funcionários:
    a. Fornecidos pelo funcionário antes ou durante a relação de emprego;
    b. Fornecidos por terceiros, como referências, informações de fornecedores ou parceiros comerciais; ou
    c. Informações disponíveis publicamente.

13. Os tipos de dados pessoais que a Empresa pode coletar, armazenar e usar sobre seus funcionários incluem registros relacionados a:
    a. endereço residencial, detalhes de contato, e detalhes de contato de parente mais próximo;
    b. informações de recrutamento, incluindo formulários de inscrição e currículos, referências recebidas e detalhes sobre qualificações;
    c. registros de pagamentos, número do cadastro de pessoa física, informações relacionadas ao pagamento de impostos, e informações relacionadas a quaisquer benefícios trabalhistas, como pensão e plano de saúde (incluindo detalhes de quaisquer pedidos de consulta ou reembolsos feitos);
    d. uso de telefone, e-mail, internet, fax ou mensagens instantâneas;

e. desempenho e quaisquer medidas disciplinares, queixas, reclamações ou questões que envolvam determinado funcionário.

14. A Empresa informa os motivos, os métodos e a hipótese legal do tratamento de seus dados pessoais. A Empresa não tratará os dados pessoais de seus funcionários por qualquer outro motivo além dos propósitos legítimos, específicos, explícitos e informados.

15. Em geral, a Empresa tratará os dados pessoais dos funcionários na administração e condução de seus negócios, incluindo, entre outros propósitos:
    a. **registros de afastamento por doença**: para manter um registro da ausência de funcionários por motivos de doença, incluindo cópias de quaisquer anotações médicas ou outros documentos fornecidos à Empresa em conexão com o pedido de afastamento ou atestado para sua saúde; para informar os colegas do funcionário afastado sobre seu afastamento; conforme necessário para gerenciar a ausência do funcionário afastado; para investigar a pedidos de ausência por doença inaceitavelmente altos ou suspeitos; para fins de avaliação da capacidade laborativa dos funcionários; para realização de pesquisas e publicação de relatórios, utilizando dados pessoais anonimizados, quanto aos níveis de afastamento por doença na Empresa.
    b. **monitoramento de sistemas corporativos de TI**: para monitorar o uso das ferramentas de trabalho como e-mails, internet, telefone e fax, computador e outras comunicações ou recursos de TI.
    c. **questões disciplinares ou legais**: para manter um registro de quaisquer questões ou procedimentos disciplinares, queixas, legais, regulamentares ou de conformidade que possam envolver os funcionários.
    d. **análises de desempenho**: para realizar análises de desempenho regulares.

16. Ocasionalmente, a Empresa poderá coletar e tratar informações pessoais sensíveis (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico) de seus funcionários. A Empresa só tratará informações pessoais sensíveis se:
    a. tiver uma hipótese legal de tratamento para fazê-lo, por exemplo, se for necessário para a execução do contrato de trabalho ou para o cumprimento de obrigação legal ou regulatória; ou
    b. o titular dos dados tiver dado seu consentimento explícito.

17. A Empresa se compromete a adotar todas as medidas razoáveis de forma a garantir que quaisquer dados pessoais tratados estejam atualizados, corretos, e sejam adequados à finalidade do tratamento.

18. Qualquer funcionário que considerar que qualquer informação mantida sobre si próprio é imprecisa ou desatualizada deve informar a situação ao EPD. Caso este concorde que as

informações são imprecisas ou desatualizadas, elas serão corrigidas imediatamente. Caso este não concorde com a correção, o funcionário será informado disto.

ARMAZENAMENTO E RETENÇÃO DE DADOS PESSOAIS

19. A Empresa se compromete a manter todos os dados pessoais (e dados pessoais sensíveis) sob seu controle em segurança e a adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

20. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, sendo conservados somente para:
    a. cumprimento de obrigação legal ou regulatória pela Empresa; ou
    b. uso exclusivo da Empresa, com a anonimização de tais dados.

DIREITOS INDIVIDUAIS DOS TITULARES DE DADOS

21. Os funcionários da Empresa e demais titulares de dados têm os seguintes direitos em relação aos seus dados tratados pela Empresa, mediante requisição:
    a. confirmação da existência de tratamento;
    b. acesso aos dados;
    c. correção de dados incompletos, inexatos ou desatualizados;
    d. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
    e. portabilidade dos dados;
    f. eliminação dos dados pessoais quando tratados com o consentimento do titular;
    g. informação das entidades públicas e privadas com as quais a Empresa realizou uso compartilhado de dados;
    h. informação sobre a possibilidade de não fornecer consentimento e sobre as consequências de tal negativa;
    i. revogação do consentimento.

22. Os titulares têm ainda o direito de peticionar em relação aos seus dados contra a Empresa perante a autoridade nacional, e o direito de se oporem a tratamento realizado sem seu consentimento, em caso de descumprimento ao disposto na LGPD.

23. Para fazer uma requisição, os titulares devem entrar em contato com o EPD via galeazzi@galeazzi.com.br.

24. A Empresa pode solicitar uma prova de identificação antes que a requisição possa ser processada. Neste caso, o requerente será avisado que será preciso verificar sua identidade e os documentos necessários.

25. Exceto em situações emergenciais, responderemos à sua solicitação dentro de 15 dias a partir da data em que sua solicitação for recebida.

26. Se a requisição for manifestamente infundada ou excessiva, a Empresa pode se recusar a cumpri-la.

SEGURANÇA DE DADOS

27. A Empresa adotará as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

28. A segurança de dados significa que a Empresa garante que:
    a. somente pessoas autorizadas a usar dados pessoais possam acessá-los;
    b. sempre que possível, os dados pessoais são pseudonimizados ou criptografados;
    c. os dados pessoais são precisos e adequados para a finalidade para a qual são tratados;
    d. as pessoas autorizadas podem acessar os dados pessoais se precisarem deles para fins autorizados.

29. Os dados pessoais não serão compartilhados com terceiros, a menos que estes terceiros tenham concordado em cumprir nossos procedimentos de segurança de dados ou demonstre à Empresa a existência e o cumprimento de outras medidas adequadas.

30. Os procedimentos de segurança da Empresa incluem:
    a. Qualquer mesa ou armário que contenha informações confidenciais deve ser mantido trancado.
    b. Os computadores devem ser bloqueados com uma senha forte que seja alterada regularmente ou desligados quando deixados sem supervisão; devem ser adotadas cautelas e discrição ao exibir dados pessoais em um monitor para garantir que estes não sejam visíveis a outras pessoas.
    c. Dados pessoais armazenados em CDs ou cartões de memória devem ser criptografados ou protegidos por senha e bloqueados com segurança quando não estiverem sendo usados.
    d. O EPD deve aprovar qualquer nuvem usada para armazenar dados.
    e. Dados pessoais nunca devem ser salvos diretamente em dispositivos móveis, como *laptops, tablets ou smartphones*.
    f. Os servidores que contêm dados pessoais devem ser mantidos em um local seguro, longe do espaço geral do escritório.

g. Todos os servidores que contêm dados pessoais sensíveis devem ser aprovados e protegidos por software de segurança.
h. O backup dos dados deve ser feito regularmente.
i. A identidade de qualquer pessoa ao telefone deve ser verificada antes da divulgação de dados pessoais. Se a identidade não puder ser verificada satisfatoriamente, a pessoa deverá ser solicitada a fazer sua consulta por escrito.
j. Cópias de dados pessoais em papel ou em qualquer dispositivo de armazenamento físico (como CDs) devem ser fisicamente destruídos quando não forem mais necessários.
k. Em caso de incerteza sobre quaisquer procedimentos, o EPD deve ser consultado.

REGISTRO DAS OPERAÇÕES E RELATÓRIO DE IMPACTO

31. A Empresa manterá registro das operações de tratamento de dados pessoais que realizar, especialmente quando baseado no legítimo interesse.

32. Em hipóteses quando o tratamento de dados pessoais puder resultar em alto risco para os direitos e liberdades do pessoal, a Empresa executará um relatório de impacto à proteção de dados pessoais para determinar a necessidade e proporcionalidade do tratamento. Isso incluirá considerar os propósitos para os quais a atividade é realizada, os riscos para os indivíduos e as medidas que podem ser adotadas para mitigar esses riscos.

VIOLAÇÕES DE DADOS

33. Caso seja descoberto algum incidente de segurança que possa acarretar risco ou dano relevante aos titulares, a Empresa comunicará tal fato, em prazo razoável, à autoridade nacional e aos titulares atingidos, informando-os ainda:
    a. a descrição da natureza dos dados pessoais afetados;
    b. as informações sobre os titulares envolvidos;
    c. as medidas técnicas e de segurança utilizadas para a proteção dos dados;
    d. os riscos relacionados ao incidente;
    e. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

34. Todos os incidentes de segurança descobertos serão registrados pela Empresa, independentemente de sua gravidade.

TREINAMENTO

35. A Empresa fornecerá regularmente treinamento a todos os indivíduos sobre suas responsabilidades de proteção de dados.

36. Indivíduos cujas tarefas exijam acesso regular a dados pessoais e/ou são responsáveis por implementar esta política e/ou responder a solicitações de acesso de titulares de acordo com essa política receberão treinamento adicional para ajudá-los a entender suas obrigações e como cumpri-las.

RESPONSABILIDADES INDIVIDUAIS

37. Os funcionários são responsáveis por ajudar o Empregador a manter seus dados pessoais atualizados e devem informar a Empresa se seus dados pessoais mudarem.

38. Funcionários que tiverem acesso a dados pessoais de outros funcionários, clientes e terceiros durante e em função da relação de emprego devem seguir as regras desta e de outras políticas internas da Empresa, bem como leis e regulamentos de proteção de dados pessoais.

39. Funcionários que tiverem acesso a dados pessoais devem:
    a. acessar apenas dados pessoais a que tenham autoridade para acessar e somente para fins autorizados;
    b. não divulgar dados pessoais, exceto para indivíduos (dentro e fora da empresa) autorizados;
    c. manter os dados pessoais em segurança, cumprindo todas as regras aplicáveis;
    d. não remover dados pessoais ou dispositivos que contenham ou possam ser usados para acessar dados pessoais das instalações da empresa sem adotar medidas de segurança apropriadas para proteger estes dados e o dispositivo; e
    e. não armazenar dados pessoais em unidades locais ou em dispositivos pessoais usados para fins profissionais.

40. Todos os funcionários vinculam-se a um dever de confidencialidade em relação a tais dados pessoais. Este compromisso de confidencialidade continuará após o término da relação de emprego.