RELATÓRIO DE LEGITIMIDADE DE INTERESSE

LIA - Legitimate Interests Assessment

Emitido em: 29/01/2025 às 11:07:33

A seguir reproduzimos todas as informações pertinentes ao tema privacidade e roteção de dados pessoais de acordo com os inventários relacionados a finalidades de tratamento de dados cujo a hipótese de tratamento de dados seja o Art. 7º, IX - Legítimo interesse do controlador. Que eve refletir os aspectos atuais do escopo da Lei Geral de Proteção de Dados.

Identificação do controlador

CNPJ: 97.676.693/0001-71

Razão Social: OMNISBLUE COMPLIANCE SERVICOS E PARTICIPACOES LTDA (Homologação)

Endereço: Santos

Website: https://www.omnisblue.com

Área de atuação: Tecnologia

Tipo de atuação: Privada

Tipo de DPO: Interno

DPO Resposável: Adilson Taub Jr

Contato do DPO: adilson.taub@omnisblue.com

Parâmetros selecionados para geração deste LIA

Diretoria: Não informado

Área: Não informado

Departamento: Não informado

Papel: Controlador

Operador: Não informado

Ativo: Não informado

Tratamento de Dados Pessoais

A seguir são listados todos os tratamentos de Dados Pessoais atualmente em execução pelo controlador, cuja hipóteses de tratamento seja Legítimo interesse, seus fundamentos legais e em quais ativos de informação esses tratamentos são realizados:

Finalidade: Envio de convites para eventos

Papel da entidade: Controlador

Trata dados sensíveis? Não

Trata dados de crianças/adolescentes?: Não

Origem da Informação: Clientes e Parceiros

Destino da Informação: Marketing

Frequência: Média (semanalmente)

Volumetria: Baixo (100 - 499)

Descrição da legitimidade de interesse

Coletar fort

Sobre os dados em tratamento

Artefatos: CPF
Lista de dados pessoais tratados na finalidade:

- Data | de emissão | Cadastral | Imprescindível para o tratamento? Não
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Não
- Número | do CPF | Cadastral | Imprescindível para o tratamento? Não

Artefatos: Registro Geral (RG)
Lista de dados pessoais tratados na finalidade:

- Data | de emissão | Cadastral | Imprescindível para o tratamento? Não
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Não
- Número | RG | Cadastral | Imprescindível para o tratamento? Não
- Orgão | expeditor | Cadastral | Imprescindível para o tratamento? Não

Artefatos: Certidão de Nascimento
Lista de dados pessoais tratados na finalidade:

- Data | de nascimento | Cadastral | Imprescindível para o tratamento? Não
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Não
- Nome | do pai | Cadastral | Imprescindível para o tratamento? Não
- Nome | da mãe | Cadastral | Imprescindível para o tratamento? Não

Sobre o processo de consentimento

O tratamento depende de consentimento: Não

Sobre operadores associados

Utiliza Operador? Sim **Operador:** Cyber Power
Dados não cadastrado

Sobre o compartilhamento de informações

Os dados são compartilhados? Não
Como os dados são compartilhados:

Não Informado

Com quem os dados são compartilhados:
Dados não cadastrado

Realiza transferências internacionais ? Não

Sobre o fim do tratamento dos dados

Os dados são descartados? Não **Prazo de armazenamento:** Não Informado
Processo de descarte:
Dados não cadastrado

Sobre os ativos de informação utilizados

Esse tratamento de dados é executado nos seguintes ativos de informação:
Ativos de informação associados ao tratamento de dados
Dados não cadastrado

Medidas administrativas de segurança

A seguir são listadas todas as medidas administrativas (políticas) atualmente em vigor na empresa, onde são documentados os compromissos do controlador com a privacidade dos Titulares de Dados Pessoais:

Política: Política de Privacidade

Tipo da política: Publica

Início de vigência: 01/01/2018 **Fim da vigência:** 31/12/2050

Responsável atual pela política: Adilson Taub Jr

Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Não **Está completa?** Não **É exequível?** Não

Trata o papel do Titular? Não **Trata o papel do DPO?** Não **Trata Operadores?** Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

Política: Política de Cookies

Tipo da política: Publica

Início de vigência: 01/01/2018 **Fim da vigência:** 31/12/2050

Responsável atual pela política: Adilson Taub Jr

Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Não **Está completa?** Não **É exequível?** Não

Trata o papel do Titular? Não **Trata o papel do DPO?** Não **Trata Operadores?** Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

Medidas técnicas de segurança

A seguir são listadas todas as medidas técnicas atualmente implementadas em cada ativo da informação utilizado para a realização de rotinas de tratamento de dados pessoais e o nível de Confiabilidade desses ativos e acordo com as atuais medidas técnicas em vigor:

Ativo da informação: Dynamics 365

Tipo do ativo: Eletrônico **Subtipo:** BPMS/Workflow

Tecnologia envolvida: SaaS **Fornecedor atual:** Cyber Power

Responsável atual pela gestão do ativo: Anderson Mattiuci

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de confidencialidade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

Nível de Integridade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de integridade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de disponibilidade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

Sobre as medidas técnicas de segurança implementadas no ativo

Medida técnica: Pseudonimização e anonimização
Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

Medida técnica: Criptografia
Proteção dos dados em trânsito e em repouso através da transformação em códigos indecifráveis sem a chave correta.

Medida técnica: Controle de acesso
Restrição do acesso aos dados pessoais apenas aos colaboradores autorizados e com necessidade de conhecer as informações. Implementação de mecanismos de autenticação e autorização robustos.

Medida técnica: Firewalls
Primeira linha de defesa: Filtra o tráfego de rede, permitindo apenas o acesso autorizado. Tipos: Firewalls de rede, de aplicativos e de próxima geração. Funcionalidades: Bloqueio de portas, inspeção de pacotes, prevenção de intrusão.

Medida técnica: Autenticação Multifator
Segurança adicional: Requer mais de uma forma de verificação de identidade, como senha, token e biometria. Tipos: Autenticação baseada em conhecimento, posse e características inerent

Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:
Riscos associados ao ativo da informação:

- Senhas fracas
- Acesso indevido ao sistema OMIE

Ativo da informação: OMIE - ERP Financeiro

Tipo do ativo: Eletrônico **Subtipo:** BPMS/Workflow

Tecnologia envolvida: Java, Oracle **Fornecedor atual:** Cyber Power

Responsável atual pela gestão do ativo: Anderson Mattiuci

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de confidencialidade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

Nível de Integridade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de integridade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de disponibilidade do serviço é gerenciada pela fornecedora que possui suas próprias

regras com relação a este serviço.

Sobre as medidas técnicas de segurança implementadas no ativo

Medida técnica: Pseudonimização e anonimização

Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

Medida técnica: Criptografia

Proteção dos dados em trânsito e em repouso através da transformação em códigos indecifráveis sem a chave correta.

Medida técnica: Controle de acesso

Restrição do acesso aos dados pessoais apenas aos colaboradores autorizados e com necessidade de conhecer as informações. Implementação de mecanismos de autenticação e autorização robustos.

Medida técnica: Firewalls

Primeira linha de defesa: Filtra o tráfego de rede, permitindo apenas o acesso autorizado. Tipos: Firewalls de rede, de aplicativos e de próxima geração. Funcionalidades: Bloqueio de portas, inspeção de pacotes, prevenção de intrusão.

Medida técnica: Autenticação Multifator

Segurança adicional: Requer mais de uma forma de verificação de identidade, como senha, token e biometria. Tipos: Autenticação baseada em conhecimento, posse e características inerent

Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:
Riscos associados ao ativo da informação:

- Senhas fracas
- Acesso indevido ao sistema OMIE

Gestão de riscos de privacidade e segurança da informação

Para a gestão de riscos de privacidade e segurança da informação, utilizamos a seguinte matriz estruturada para classificação da criticidade de cada risco, que é composta de acordo com a classificação de impacto do risco e sua probabilidade percentual em ocorrer:

		Impacto		
		Baixo	Média	Alto
Probabilidade	100%	Alta	Urgente	Urgente
	90%	Moderada	Urgente	Urgente
	80%	Moderada	Alta	Urgente
	70%	Moderada	Alta	Urgente
	60%	Moderada	Alta	Alta
	50%	Baixa	Alta	Alta
	40%	Baixa	Moderada	Alta
	30%	Baixa	Moderada	Moderada
	20%	Baixa	Baixa	Moderada
	10%	Baixa	Baixa	Moderada

A seguir são listados todos os atuais riscos de privacidade e proteção de dados identificados e que estão sendo gerenciados pelo controlador, ordenados de acordo com sua criticidade:

Dados não cadastrado