

POLÍTICA INTERNA

PLT-USC-0001

Política Geral de Proteção de Dados / General Data Protection Regulation Policy

Vigência / Effective 15/03/2024
Revisão / Revision 01

Alterações desta revisão / Changes from this review
Análise crítica do conteúdo / Critical content analysis

Revisões anteriores / Previous reviews
Da / From 00 (04/02/2022)
Elaboração desta política / Preparation of this policy


Analisado criticamente e aprovado por: / Critically reviewed and approved by:

**Gerente da Qualidade e Assuntos Regulatórios / Quality and Regulatory Affairs
Manager**


Visto: / Check:

SUMÁRIO / TABLE OF CONTENTS

Item	Pág. / Page
Objetivo / Objective.....	4
Descrição / Description.....	4
Introdução / Introduction	4
Declaração de política / Policy statement	4
Status / Status	4
Escopo / Scope	5
A quem se aplica / Who it applies to	5
Por que e como se aplica a eles / Why and how it applies to them	5
Definição dos termos / Definition of terms	5
Proteção de dados por projeto e padrão / Data protection by design and default.....	5
Comitê de Proteção de Dados / Data Protection Committee	6
Controlador de dados / Data controller	6
Processador de dados / Data processor	6
Titular dos dados / Data subject.....	6
Dados pessoais / Personal data.....	7
Processamento / Processing.....	7
Pseudonimização / Pseudonymisation.....	7
Destinatário / Recipient	7
Proteção de dados por projeto e padrão / Data protection by design and default	8
Proteção de dados por projeto / Data protection by design	8
Proteção de dados por padrão / Data protection by default.....	9
Papéis dos controladores e processadores de dados / Roles of data controllers and processors	10
Controlador de dados / Data controller	10
Processador de dados / Data processor.....	12
Dados incorretos / Incorrect data.....	14
Visão geral / Overview.....	14
Direito de ser informado / Right to be informed.....	14
Direito de acesso / Right of access	15
Direito de retificação / Right to rectification	15
Direito de apagar / Right to erasure	16
Direito de restringir o processamento / Right to restrict processing.....	16
Direito à portabilidade de dados / Right to data portability.....	16
Direito de oposição / Right to object.....	17
Direitos em relação à tomada de decisão automatizada e criação de perfil / Rights in relation to automated decision making and profiling	17
Solicitações de acesso do titular / Subject access requests	17

	PLT-USC-0001	Pág. 3 de 33 / Page 3 of 33
	Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Vig. / Eff. 15/03/2024
		Revisão / Revision 01

Reconhecendo as solicitações de acesso do titular / Recognising subject access requests	17
Respondendo a uma solicitação de acesso do titular / Responding to a subject access request.....	18
Taxas / Fees	18
Verificando a solicitação de acesso do titular / Verifying the subject access request	18
Fornecimento das informações solicitadas / Supplying the requested information	18
Solicitações de terceiros / Third party requests	19
Solicitações de advogados / Requests from solicitors	19
Recusando-se a cumprir uma solicitação / Refusing to comply with a request	19
Violação de dados / Data breaches	20
Definição de violação de dados / Data breach definition	20
Relatando uma violação de dados / Reporting a data breach	21
Notificar um titular de dados sobre uma violação / Notifying a data subject of a breach	22
Consentimento / Consent.....	23
Adequação / Appropriateness	23
Obtenção de consentimento / Obtaining consent	23
Consentimento dos pais / Parental consent.....	24
Mapeamento dos dados e avaliações de impacto de proteção de dados / Data mapping and Data Protection Impact Assessments	24
Mapeamento dos dados / Data mapping	24
Mapeamento de dados e avaliação de impacto na proteção de dados / Data mapping and the Data Protection Impact Assessment.....	25
Avaliação do impacto da proteção de dados / Data protection impact assessment.....	26
Proc. de avaliação de impacto da proteção de dados / Data Protection Impact Assessment process	27
Anexos	28

	PLT-USC-0001	Pág. 4 de 33 / Page 4 of 33
	Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Vig. / Eff. 15/03/2024
		Revisão / Revision 01

1. OBJETIVO / OBJECTIVE

Definir as principais regras de proteção aos dados pessoais, no que se refere a todos os processos da Braile Biomédica.

Define the main rules for the protection of personal data, with regard to all processes of Braile Biomédica.

2. DESCRIÇÃO / DESCRIPTION

2.1 Introdução / Introduction

2.1.1 Declaração de política / Policy statement

A Braile Biomédica se compromete a atender aos requisitos pertinentes da Lei Geral de Proteção de Dados (LGPD) e a General Data Protection Regulation (GDPR), no que diz respeito a todas suas relações enquanto fabricante de produtos para a saúde, na interação com outros atores, serviços de saúde e pacientes/usuários.


O compromisso e atendimento aos requisitos garante que todos os dados pessoais de quaisquer stakeholders estarão protegidos.

Braile Biomédica undertakes to comply with the relevant requirements of the General Data Protection Act (LGPD) and the General Data Protection Regulation (GDPR), with regard to all its relationships as a manufacturer of health products, in the interaction with other actors, health services and patients/users.

Commitment to and compliance with requirements ensures that all personal data of any stakeholders will be protected.

2.1.2 Status / Status

A Braile Biomédica visa conceber e implementar políticas e procedimentos que respondam às diversas necessidades do nosso serviço e força de trabalho, garantindo que nenhum seja colocado em desvantagem em relação aos outros. Foi considerado o impacto que esta política pode ter em relação às características individuais protegidas daqueles a quem ela se aplica.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 5 de 33 / Page 5 of 33
		Vig. / Eff. 15/03/2024
	Revisão / Revision 01	

The organization aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others. Consideration has been given to the impact this policy might have regarding individual protected characteristics of those to whom it applies.

2.2 Escopo / Scope

2.2.1 A quem se aplica / Who it applies to

Este documento aplica-se a todos os colaboradores, parceiros e clientes da Braile Biomédica. Além disso, também se aplica a médicos que trabalham sob qualquer tipo de contrato.

This document applies to all employees, partners and clients of Braile Biomédica. Furthermore, it also applies to clinicians who are working under any kind of contracts.

2.2.2 Por que e como se aplica a eles / Why and how it applies to them


Todo o pessoal da Braile Biomédica tem a responsabilidade de proteger as informações que processa. Este documento foi produzido para permitir que todos os funcionários entendam suas responsabilidades individuais e coletivas em relação à LGPD e ao GDPR.

All personnel at Braile Biomédica have a responsibility to protect the information they process. This document has been produced to enable all staff to understand their individual and collective responsibilities in relation to the LGPD and to the GDPR.

2.3 Definição dos termos / Definition of terms

2.3.1 Proteção de dados por projeto e padrão / Data protection by design and default

A proteção de dados desde o projeto demanda a implementação de medidas técnicas e organizacionais adequadas para implementar os princípios de proteção de dados de forma eficaz e salvaguardar os direitos individuais.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 6 de 33 / Page 6 of 33
		Vig. / Eff. 15/03/2024
	Revisão / Revision 01	

Data protection by design requires the implementation of appropriate technical and organizational measures to effectively implement data protection principles and safeguard individual rights.

2.3.2 Comitê de Proteção de Dados / Data Protection Committee

Um comitê de especialistas em privacidade de dados, trabalhando de forma independente para garantir a conformidade com as políticas e procedimentos.

An expert committee on data privacy, working independently to ensure compliance with policies and procedure.

2.3.3 Controlador de dados / Data controller

A pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outros, determine as finalidades e os meios de tratamento dos dados pessoais.

The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.

2.3.4 Processador de dados / Data processor


Uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que processa dados pessoais em nome do controlador.

A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

2.3.5 Titular dos dados / Data subject

O indivíduo vivo identificado ou identificável a quem os dados pessoais se referem.

The identified or identifiable living individual to who personal data relates.

	PLT-USC-0001	Pág. 7 de 33 / Page 7 of 33
	Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Vig. / Eff. 15/03/2024
		Revisão / Revision 01

2.3.6 Dados pessoais / Personal data

Informações relacionadas a um indivíduo identificado ou identificável.

Information that relates to an identified or identifiable individual.

2.3.7 Processamento / Processing

Qualquer operação ou conjunto de operações que seja realizada sobre dados pessoais ou sobre conjuntos de dados pessoais, seja por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição ou destruição.

Any operation or set of operations that is performed on personal data or on sets of personal data whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or destruction.

2.3.8 Pseudonimização / Pseudonymisation


A pseudonimização é uma técnica que substitui ou remove informações em um conjunto de dados que identifica um indivíduo.

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.

2.3.9 Destinatário / Recipient

A entidade a quem os dados pessoais são divulgados.

The entity to which personal data is disclosed.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 8 de 33 / Page 8 of 33
		Vig. / Eff. 15/03/2024
	Revisão / Revision 01	

2.4 Proteção de dados por projeto e padrão / Data protection by design and default

2.4.1 Proteção de dados por projeto / Data protection by design

A proteção de dados desde o projeto é, em última análise, uma abordagem que garante que as questões de privacidade e proteção de dados sejam consideradas na fase de projeto de qualquer sistema, serviço, produto ou processo e, em seguida, durante todo o ciclo de vida.


Data protection by design is ultimately an approach that ensures that privacy and data protection issues are considered at the design phase of any system, service, product or process and then throughout the lifecycle.

A Braille Biomédica demonstrará a proteção de dados desde o projeto:

- Pela realização de uma avaliação de impacto de proteção de dados;
- Pela garantia de que haja aviso de privacidade no site escrito em linguagem simples e fácil de entender;
 - Implementando medidas técnicas e organizacionais adequadas que se destinam a aplicar os princípios de proteção de dados, como a minimização de dados, de forma eficaz e a integrar as salvaguardas necessárias no tratamento, a fim de proteger os direitos dos titulares dos dados;
 - Implementando medidas técnicas e organizacionais adequadas para garantir que apenas os dados pessoais necessários para cada finalidade específica do processamento sejam processados.
 - Aderindo à Seção 2.5.1 desta política.

Braille Biomédica will demonstrate data protection by design:

- By conducting a data protection impact assessment;
- By ensuring that there are privacy notice on the website which are written in simple, easy-to-understand language;
 - Implementing appropriate technical and organisational measures which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to protect the rights of data subjects;

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 9 de 33 / Page 9 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

- Implementing appropriate technical and organisational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are processed;

- Adhering to Section 2.5.1 of this policy.

A proteção de dados por design é um requisito legal.

Data protection by design is a legal requirement.

2.4.2 Proteção de dados por padrão / Data protection by default

A proteção de dados por padrão é uma abordagem que garante que os dados sejam processados apenas para a realização de uma finalidade específica.


Data protection by default is an approach that ensures that data is processed only for the achievement of a specific purpose.

A Braille Biomédica demonstrará a proteção de dados por padrão:

- Pelo processamento de dados apenas para a(s) finalidade(s) pretendida(s);
- Pela Garantia de que o consentimento seja obtido do titular dos dados antes do processamento dos dados;
- Pelo fornecimento ao solicitante o acesso aos seus dados mediante solicitação;
- Pelo processamento de dados de forma a evitar que os titulares dos dados sejam identificados, a menos que sejam fornecidas informações adicionais (usando referências em vez de nomes - pseudonimização);
- Pelo processamento de dados de acordo com a seção 2.5.2 desta política.

Braille Biomédica will demonstrate data protection by default by:

- By processing data only for the purpose(s) intended;
- By ensuring consent is obtained from the data subject prior to data being processed;
- By providing the requester the access his own data by request;
- By processing data in a manner that prevents data subjects being identified unless additional information is provided (using references as opposed to names – pseudonymisation);
- By processing data in accordance with section 2.5.2 of this policy.

	PLT-USC-0001	Pág. 10 de 33 / Page 10 of 33
	Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Vig. / Eff. 15/03/2024
		Revisão / Revision 01

2.5 Papéis dos controladores e processadores de dados / Roles of data controllers and processors


2.5.1 Controlador de dados / Data controller

Na Braille Biomédica, o papel do controlador de dados é garantir que os dados sejam processados de acordo com a LGPD. A empresa deve ser capaz de demonstrar conformidade e é responsável por garantir que os dados sejam:

- Processados de forma legal, justa e transparente em relação ao titular dos dados;
- Coletados para fins específicos, explícitos e legítimos e não processados de maneira incompatível com esses fins;
- Adequados, relevantes e limitados ao necessário em relação às finalidades para as quais os dados são processados;
- Exatos e, quando necessário, atualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados pessoais inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora;
- Mantidos de uma forma que permita a identificação dos titulares dos dados por não mais do que o necessário para os fins para os quais os dados pessoais são processados;
- Processados de maneira a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas.

At Braille Biomédica, the role of the data controller is to ensure that data is processed in accordance with GDPR. The company should be able to demonstrate compliance and is responsible for making sure that data is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 11 de 33 / Page 11 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data, which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

A Braile Biomédica é a controladora de dados e, como tal, os parceiros são responsáveis por garantir que todos os processadores de dados cumpram esta política e a LGPD.


Braile Biomédica is the data controller and as such the partners are responsible for ensuring that all data processors comply with this policy and the GDPR.

O responsável pela proteção de dados (DPO) da Braile Biomédica é o Comitê LGPD composto por:

- Caroline Barbarotti – analista departamento pessoal
- Diego Silvério – gerente financeiro
- Enio Shiota – advogado
- Gláucia Basso – coordenadora de pesquisa
- Giovana Guizzo – coordenadora comercial
- Carlos M. Kanashiro – gerente de TI
- Rosângela Miranda – assessoria da presidência
- Sandro Ottoboni – gerente da qualidade/assuntos regulatórios
- Sílvia Machado – coordenadora de acesso ao mercado

The data protection officer (DPO) for Braile Biomédica is the GDPR Committee composed of:

- Caroline Barbarotti – personnel department analyst
- Diego Silvério – financial manager
- Enio Shiota – lawyer
- Gláucia Basso – research coordinator
- Giovana Guizzo - commercial coordinator

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 12 de 33 / Page 12 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

- Carlos M. Kanashiro – IT Manager
- Rosângela Miranda – presidency advisory
- Sandro Ottoboni – quality/regulatory affairs manager
- Sílvia Machado – market access coordinator

O Comitê está disponível para fornecer aconselhamento de proteção de dados e suporte às práticas durante o horário normal de trabalho para ajudar a garantir a conformidade com o LGPD.

The Committee is available to provide data protection advice and support to practices during normal working hours to help ensure compliance with the GDPR.

O suporte incluirá obrigações de conformidade com a legislação de proteção de dados, solicitações de acesso/direitos do sujeito, aconselhamento quando as avaliações de impacto de proteção de dados são necessárias, fornecimento de documentação e orientação sobre sua conclusão, conforme necessário, conscientização da equipe e aconselhamento sobre Avisos de Privacidade.

O contato do Comitê é privacidade@braile.com.br


The support will include compliance obligations with data protection legislation, subject access/rights requests, advising when data protection impact assessments are required, providing documentation and guidance on its completion as necessary, staff awareness and advice around Privacy Notices.

The contact of the Committee is privacidade@braile.com.br

2.5.2 Processador de dados / Data processor

Os processadores de dados são responsáveis pelo processamento de dados pessoais em nome do controlador de dados. Os processadores devem garantir que o processamento seja legal e que pelo menos um dos seguintes se aplique:

- O titular dos dados deu consentimento para o processamento de seus dados pessoais para uma ou mais finalidades específicas;
- O processamento é necessário para a execução de um contrato do qual o titular dos dados é parte ou para tomar medidas a pedido do titular dos dados antes de celebrar um contrato;


	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 13 de 33 / Page 13 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

- O processamento é necessário para o cumprimento de uma obrigação legal a que o controlador de dados está sujeito;
- O processamento é necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa física;
- O processamento é necessário para o desempenho de uma tarefa realizada no interesse público ou no exercício de autoridade oficial investida no controlador de dados;
- O tratamento é necessário para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por um terceiro, exceto quando tais interesses se sobrepõem aos interesses ou direitos e liberdades fundamentais do titular dos dados que exijam proteção de dados pessoais, em particular quando o titular dos dados é uma criança.

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful and that at least one of the following applies:

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the data controller is subject;
- Processing is necessary in order to protect the vital interests of the data subject or another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Na Braille Biomédica, todos os funcionários são classificados como processadores de dados, pois suas funções individuais exigirão que eles acessem e processem dados pessoais.

	PLT-USC-0001	Pág. 14 de 33 / Page 14 of 33
	Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Vig. / Eff. 15/03/2024
		Revisão / Revision 01

At Braile Biomédica, all staff are classed as data processors as their individual roles will require them to access and process personal data.

2.6 Dados incorretos / Incorrect data

2.6.1 Visão geral / Overview

Todos os titulares dos dados têm os seguintes direitos:


1. O direito de ser informado;
2. O direito de acesso;
3. O direito de retificação;
4. O direito de apagar;
5. O direito de restringir o processamento;
6. O direito à portabilidade de dados;
7. O direito de oposição;
8. Direitos em relação à tomada de decisão automatizada e criação de perfil.

All data subjects have the following rights:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

2.6.2 Direito de ser informado / Right to be informed

A Braile Biomédica é obrigada a informar os titulares dos dados sobre as finalidades do processamento de seus dados, os períodos de retenção dos dados e com quem esses dados serão compartilhados. Isso é conhecido como informações de privacidade.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 15 de 33 / Page 15 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

Braile Biomédica is obliged to advise data subjects of the purposes for processing their data, the retention periods for the data and who this data will be shared with. This is referred to as privacy information.

2.6.3 Direito de acesso / Right of access

A Braile Biomédica garante que todos estejam cientes de seu direito de acesso aos seus dados.

Braile Biomédica guarantees that everyone is aware of their right to access their data.

Para cumprir o LGPD, todos os avisos de privacidade da organização são escritos em uma linguagem compreensível para todos e atendem aos critérios detalhados do LGPD.


O motivo da concessão de acesso aos titulares dos dados é permitir-lhes verificar a licitude do tratamento dos dados sobre eles detidos. Além disso, os titulares dos dados podem autorizar o acesso de terceiros de acordo com a LGPD.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorize third party access under the GDPR.

2.6.4 Direito de retificação / Right to rectification

De acordo com a LGPD, os titulares de dados têm o direito de ter dados pessoais imprecisos retificados e/ou dados pessoais incompletos preenchidos.

In accordance with the GDPR, data subjects have the right to have inaccurate personal data rectified and/or incomplete personal data completed.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 16 de 33 / Page 16 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

2.6.5 Direito de apagar / Right to erasure

De acordo com a LGPD, os titulares de dados têm o direito de apagar os dados pessoais. Este direito permite que um titular de dados solicite que os dados pessoais sejam excluídos em situações em que não haja motivo convincente para reter os dados.

In accordance with GDPR, data subjects have the right to have personal data erased. This right permits a data subject to request personal data is deleted in situations where there is no compelling reason to retain the data.

Quando a Braile Biomédica compartilha informações com terceiros, há a obrigação de informar o terceiro sobre a solicitação do titular dos dados para apagar seus dados, desde que seja viável e razoavelmente prático fazê-lo.

Where Braile Biomédica share information with a third party, there is an obligation to inform the third party about the data subject's request to erase their data providing it is achievable and reasonably practical to do so.

2.6.6 Direito de restringir o processamento / Right to restrict processing


De acordo com a LGPD, os indivíduos têm o direito de restringir o processamento de seus dados pessoais. Isso se aplica em determinadas circunstâncias, com o objetivo de permitir que o indivíduo limite a maneira como uma organização processa (usa) seus dados. Este direito pode ser utilizado como alternativa ao direito ao apagamento.

In accordance with GDPR, individuals have the right to restrict the processing of their personal data. This applies in certain circumstances, with the aim being to enable the individual to limit the way an organisation processes (uses) their data. This right can be used as an alternative to the right to erasure.

2.6.7 Direito à portabilidade de dados / Right to data portability

O direito à portabilidade de dados permite que os titulares de dados recebam e reutilizem seus dados pessoais para seus próprios fins e em diferentes serviços.

The right to data portability permits data subjects to receive and reuse their personal data for their own purposes and across different services.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 17 de 33 / Page 17 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

2.6.8 Direito de oposição / Right to object

De acordo com a LGPD, os indivíduos têm o direito de se opor ao processamento de seus dados pessoais a qualquer momento. Na Braile Biomédica, os indivíduos são solicitados a fornecer motivos específicos pelos quais se opõem ao processamento de seus dados. Se os motivos não forem um direito absoluto, a Braile Biomédica pode se recusar a cumprir.

In accordance with GDPR, individuals have the right to object to the processing of their personal data at any time. At Braile Biomédica, individuals are requested to provide specific reasons why they object to the processing of their data. If the reasons are not an absolute right, Braile Biomédica can refuse to comply.

2.6.9 Direitos em relação à tomada de decisão automatizada e criação de perfil / Rights in relation to automated decision making and profiling

De acordo com a LGPD, a Braile Biomédica não tem permissão para tomar decisões exclusivamente automatizadas. Isso inclui perfis.


In accordance with GDPR, Braile Biomédica, is not permitted to make solely automated decision making. This includes profiling.

2.7 Solicitações de acesso do titular / Subject access requests

2.7.1 Reconhecendo as solicitações de acesso do titular / Recognising subject access requests

Na Braile Biomédica, os titulares dos dados são incentivados a solicitar os dados necessários. Quaisquer solicitações devem ser processadas.

At Braile Biomédica, data subjects are encouraged to request necessary data. Any requests must be processed.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 18 de 33 / Page 18 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

2.7.2 Respondendo a uma solicitação de acesso do titular / Responding to a subject access request

De acordo com a LGPD, os controladores de dados devem responder a todas as solicitações de acesso do titular dos dados.

In accordance GDPR, data controllers must respond to all data subject access requests.

2.7.3 Taxas / Fees

De acordo com a LGPD, a Braile Biomédica não pode cobrar dos titulares dos dados pelo acesso inicial; isso deve ser feito gratuitamente.

Under the GDPR, Braile Biomédica is not permitted to charge data subjects for initial access; this must be done free of charge.


2.7.4 Verificando a solicitação de acesso do titular / Verifying the subject access request

É responsabilidade do controlador de dados verificar todas as solicitações dos titulares dos dados usando medidas razoáveis. O controlador de dados pode solicitar provas para identificar o titular dos dados.

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures. The data controller is permitted to ask for evidence to identify the data subject.

2.7.5 Fornecimento das informações solicitadas / Supplying the requested information

A decisão sobre qual formato fornecer as informações solicitadas deve levar em consideração as circunstâncias da solicitação e se o indivíduo pode acessar os dados no formato fornecido.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 19 de 33 / Page 19 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

The decision on what format to provide the requested information in should take into consideration the circumstances of the request and whether the individual can access the data in the format provided.

2.7.6 Solicitações de terceiros / Third party requests

Na Braile Biomédica, o controlador de dados deve poder certificar-se de que a pessoa que solicita os dados possui a autoridade do titular dos dados.

At Braile Biomédica, the data controller must be able to satisfy themselves that the person requesting the data has the authority of the data subject.

A responsabilidade de fornecer a autoridade necessária é do terceiro e geralmente é na forma de uma declaração por escrito ou formulário de consentimento, assinado pelo titular dos dados.

The responsibility for providing the required authority rests with the third party and is usually in the form of a written statement or consent form, signed by the data subject.

2.7.7 Solicitações de advogados / Requests from solicitors


Na Braile Biomédica, são recebidas solicitações de terceiros, como solicitadores. É responsabilidade do terceiro fornecer evidências de que eles têm permissão para solicitar em nome de seu cliente.

At Braile Biomédica, requests are received from third parties such as solicitors. It is the responsibility of the third party to provide evidence that they are permitted to request on behalf of their client.

2.7.8 Recusando-se a cumprir uma solicitação / Refusing to comply with a request

A Braile Biomédica somente se recusará a atender uma solicitação quando houver isenção ou quando a solicitação for manifestamente infundada ou manifestamente excessiva. Em tais situações, o controlador de dados informará o indivíduo sobre:

- As razões pelas quais o pedido foi recusado;
- Sua capacidade de buscar a aplicação deste direito através dos tribunais.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 20 de 33 / Page 20 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

Braile Biomédica will only refuse to comply with a request where exemption applies or when the request is manifestly unfounded or manifestly excessive. In such situations, the data controller will inform the individual of:

- The reasons why the request was refused;
- Their ability to seek enforcement of this right through the courts.

Cada solicitação deve ser cuidadosamente considerada e caso a Braile Biomédica se recuse a atender, isso deve ser registrado e os motivos da recusa justificáveis.

Each request must be given careful consideration and should Braile Biomédica refuse to comply, this must be recorded and the reasons for refusal justifiable.

2.8 Violação de dados / Data breaches


2.8.1 Definição de violação de dados / Data breach definition

Uma violação de dados é definida como um incidente de segurança que afetou a confidencialidade, integridade ou disponibilidade de dados pessoais. Exemplos de violações de dados incluem:

- Acesso por terceiros não autorizados;
- Ação deliberada ou acidental (ou inação) por um controlador de dados ou processador;
- Envio de dados pessoais para um destinatário incorreto;
- Perda ou roubo de dispositivos de computador contendo dados pessoais;
- Alteração de dados pessoais sem permissão;
- Perda de disponibilidade de dados pessoais.

A data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Examples of data breaches include:

- Access by an unauthorized third party;
- Deliberate or accidental action (or inaction) by a data controller or processor;
- Sending personal data to an incorrect recipient;
- Loss or theft of computer devices containing personal data;
- Alteration of personal data without permission;
- Loss of availability of personal data.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 21 de 33 / Page 21 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

2.8.2 Relatando uma violação de dados / Reporting a data breach

Na Braille Biomédica, caso algum membro da equipe tome conhecimento de uma violação de dados, ele deve, sempre que possível, conter a violação e avisar o Comitê de GDPR imediatamente.

At Braille Biomédica, should any member of staff become aware of a data breach, they are, where possible, to contain the breach and advise the GDPR Committee immediately.

Ao determinar se a Braille Biomédica precisa denunciar a violação de dados, essa decisão deve ser baseada se a violação é ou não um alto risco para os direitos e liberdades de um indivíduo.

When determining whether Braille Biomédica needs to report the data breach, this decision is to be based on whether or not the breach is a high risk to an individual's rights and freedoms.

As violações devem ser relatadas sem demora injustificada de tomar conhecimento da violação.


Breaches are to be reported without undue delay of becoming aware of the breach.

O controlador de dados deve garantir que todas as violações na Braille Biomédica sejam registradas. A LGPD descreve os requisitos que incluem:

- Registros dos fatos relativos à violação;
- Os efeitos que a violação teve em indivíduos ou organizações;
- Quaisquer ações corretivas que tenham sido concluídas;
- A causa da violação, ou seja, sistema ou erro humano;
- Considerar quais mudanças de sistema ou processo podem ser necessárias para evitar futuras incidências.

The data controller is to ensure that all breaches at Braille Biomédica are recorded. GDPR outlines the requirements which include:

- Records of the facts pertaining to the breach;
- The effects the breach has had on individuals or organizations;
- Any remedial action(s) that have been completed;

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 22 de 33 / Page 22 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

- The cause of the breach i.e., system or human error;
- Considering what system or process changes may be required to prevent future incidences.

2.8.3 Notificar um titular de dados sobre uma violação / Notifying a data subject of a breach

O controlador de dados deve notificar o titular dos dados sobre uma violação que afetou seus dados pessoais sem demora injustificada. A principal razão para notificar um titular de dados de uma violação é dar-lhe a oportunidade de tomar as medidas necessárias para se proteger dos efeitos de uma violação.


The data controller must notify a data subject of a breach that has affected their personal data without undue delay. The primary reason for notifying a data subject of a breach is to afford them the opportunity to take the necessary steps in order to protect themselves from the effects of a breach.

Quando for tomada a decisão de notificar um titular de dados sobre uma violação, o controlador de dados da Braile Biomédica deve fornecer ao titular dos dados as seguintes informações de forma clara e compreensível:

- As circunstâncias que cercam a violação;
- Os detalhes da pessoa que gerenciará a violação;
- Quaisquer ações tomadas para conter e gerenciar a violação;
- Qualquer outra informação pertinente para apoiar o titular dos dados.

When the decision has been made to notify a data subject of a breach, the data controller at Braile Biomédica is to provide the data subject with the following information in a clear, comprehensible manner:

- The circumstances surrounding the breach;
- The details of the person who will be managing the breach;
- Any actions taken to contain and manage the breach;
- Any other pertinent information to support the data subject.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 23 de 33 / Page 23 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

2.9 Consentimento / Consent

2.9.1 Adequação / Appropriateness

A LGPD afirma que o consentimento deve ser inequívoco e requer uma ação positiva para “aceitar” e deve ser dado livremente. Os titulares dos dados têm o direito de retirar o consentimento a qualquer momento.

The GDPR states that consent must be unambiguous and requires a positive action to “opt in” and it must be freely given. Data subjects have the right to withdraw consent at any time.

2.9.2 Obtenção de consentimento / Obtaining consent

O consentimento é uma das bases legais de processamento e é apropriado se os processadores de dados estiverem em posição de “oferecer às pessoas escolha e controle reais sobre como seus dados são usados”. Se for considerado adequado obter o consentimento, deve ser explicado ao titular dos dados o seguinte:


- Por que a organização deseja os dados;
- Como os dados serão usados pela organização;
- Os nomes de quaisquer controladores de dados de terceiros com os quais os dados serão compartilhados;
- Seu direito de retirar o consentimento a qualquer momento.

Consent is one of the lawful bases of processing and is appropriate if data processors are in a position to “offer people real choice and control over how their data is used”. If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

- Why the organization wants the data;
- How the data will be used by the organization;
- The names of any third party data controllers with whom the data will be shared;
- Their right to withdraw consent at any time.

Todos os pedidos de consentimento devem ser registrados, com o registro mostrando:

- Os detalhes do consentimento do titular dos dados;
- Quando eles consentiram;

	PLT-USC-0001	Pág. 24 de 33 / Page 24 of 33
	Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Vig. / Eff. 15/03/2024
		Revisão / Revision 01

- Como eles consentiram;
- Quais informações o titular dos dados foi informado.

All requests for consent are to be recorded, with the record showing:

- The details of the data subject consenting;
- When they consented;
- How they consented;
- What information the data subject was told.

O consentimento deve ser claramente identificável. Além disso, o controlador de dados deve garantir que os titulares dos dados estejam plenamente cientes de seu direito de retirar o consentimento e deve facilitar a retirada conforme e quando solicitado.

Consent is to be clearly. Furthermore, the data controller must ensure that data subjects are fully aware of their right to withdraw consent and must facilitate withdrawal as and when it is requested.

2.9.3 Consentimento dos pais / Parental consent

O consentimento dos pais (em relação a dados pessoais) é necessário para uma criança.


Parental consent (in relation to personal data) is required for a child.

2.10 Mapeamento dos dados e avaliações de impacto de proteção de dados / Data mapping and Data Protection Impact Assessments

2.10.1 Mapeamento dos dados / Data mapping

O mapeamento de dados é um meio de determinar o fluxo de informações em toda a organização. Entender o porquê, quem, o quê, quando e onde do caminho da informação permitirá à Braille Biomédica realizar uma avaliação completa dos riscos associados aos processos de dados atuais.

Data mapping is a means of determining the information flow throughout an organization. Understanding the why, who, what, when and where of the information

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 25 de 33 / Page 25 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

pathway will enable Braile Biomédica to undertake a thorough assessment of the risks associated with current data processes.

O mapeamento de dados eficaz identificará quais dados estão sendo processados, o formato dos dados, como estão sendo transferidos, se os dados estão sendo compartilhados e onde estão armazenados (incluindo armazenamento externo, se aplicável).

Effective data mapping will identify what data is being processed, the format of the data, how it is being transferred, if the data is being shared and where it is stored (including off-site storage if applicable).

O Anexo A (3.1) detalha o processo de mapeamento de dados na Braile Biomédica.

Annex A (3.1) details the process of data mapping at Braile Biomédica.


2.10.2 Mapeamento de dados e avaliação de impacto na proteção de dados / Data mapping and the Data Protection Impact Assessment

O mapeamento de dados está vinculado à avaliação de impacto na proteção de dados e, quando o elemento de análise de risco do processo é realizado, as informações apuradas durante o processo de mapeamento podem ser utilizadas.

Data mapping is linked to the data protection impact assessment and, when the risk analysis element of the process is undertaken, the information ascertained during the mapping process can be used.

Todos os funcionários da Braile Biomédica estarão envolvidos no processo de mapeamento, permitindo assim a coleta mais ampla de informações precisas.

All staff at Braile Biomédica will be involved in the mapping process thus enabling the wider gathering of accurate information.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 26 de 33 / Page 26 of 33
		Vig. / Eff. 15/03/2024
	Revisão / Revision 01	

2.10.3 Avaliação do impacto da proteção de dados / Data protection impact assessment

A avaliação do impacto da proteção de dados é a forma mais eficiente para a Braile Biomédica cumprir suas obrigações de proteção de dados e as expectativas de seus titulares de dados.

The data protection impact assessment is the most efficient way for Braile Biomédica to meet its data protection obligations and the expectations of its data subjects.

De acordo com a LGPD, uma avaliação do impacto da proteção de dados deve ser realizada quando:


- Um tipo de processamento, em particular usando novas tecnologias, e levando em consideração a natureza, escopo, contexto e finalidades do processamento, pode resultar em alto risco para os direitos e liberdades das pessoas físicas, o controlador deve, antes ao tratamento, proceder a uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais;
- Extensas atividades de processamento são realizadas, incluindo processamento em larga escala de dados pessoais e/ou especiais.

In accordance with GDPR, a data protection impact assessment should be undertaken where:

- A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data;
- Extensive processing activities are undertaken, including large scale processing of personal and/or special data;

As avaliações do impacto da proteção de dados devem incluir o seguinte:

- Uma descrição das operações de processamento, incluindo a finalidade do processamento;
- Uma avaliação da necessidade do processamento em relação à finalidade;
- Uma avaliação dos riscos associados aos titulares dos dados;
- Medidas existentes para mitigar e controlar o(s) risco(s);
- Evidência de conformidade em relação ao controle de risco.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 27 de 33 / Page 27 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

Data protection impact assessments are to include the following:

- A description of the processing operations, including the purpose of processing;
- An evaluation of the need for the processing in relation to the purpose;
- An assessment of the associated risks to the data subjects;
- Existing measures to mitigate and control the risk(s);
- Evidence of compliance in relation to risk control.

As avaliações do impacto da proteção de dados são classificadas como “documentos ativos” e os processos devem ser revisados continuamente. No mínimo deve ser revisto a cada três anos ou sempre que houver uma mudança em um processo que envolva dados pessoais.

Data protection impact assessments are classed as “live documents” and processes should be reviewed continually. As a minimum should be reviewed every three years or whenever there is a change in a process that involves personal data.


2.10.4 Processo de avaliação de impacto da proteção de dados / Data Protection Impact Assessment process

O processo é um ciclo como definido abaixo:

1. Identificar a necessidade de avaliação do impacto da proteção de dados;
2. Descrever o processamento;
3. Considere a consulta;
4. Avaliar a necessidade e a proporcionalidade;
5. Identificar e avaliar os riscos;
6. Identificar medidas para mitigar o risco;
7. Assine e registre os resultados;
8. Integre os resultados ao plano;
9. Manter sob revisão.

The process is a cycle as defined below:

1. Identify need for data protection impact assessment;
2. Describe the processing;
3. Consider consultation;
4. Assess necessity and proportionality;
5. Identify and assess risks;

	PLT-USC-0001	Pág. 28 de 33 / Page 28 of 33
	Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Vig. / Eff. 15/03/2024
		Revisão / Revision 01

6. Identify measures to mitigate risk;
7. Sign off and record outcomes;
8. Integrate outcomes into plan;
9. Keep under review.


O Anexo B (3.2) fornece um modelo que deve ser usado para realizar uma avaliação do impacto da proteção de dados na Braile Biomédica.

Annex B (3.2) provides a template that is to be used to carry out a data protection impact assessment at Braile Biomédica.


3. ANEXOS

3.1 Anexo A – O processo de mapeamento de dados / Annex A – The data mapping process

3.2 Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 29 de 33 / Page 29 of 33
		Vig. / Eff. 15/03/2024
	Revisão / Revision 01	

3.1 Anexo A – O processo de mapeamento de dados / Annex A – The data mapping process

	Anexo A – O processo de mapeamento de dados / Annex A – The data mapping process	Pág. 1 de 1 / Page 1 of 1
		Data / Date:

PLT-USC-0001	REVISÃO / REVISION
---------------------	---------------------------

**Mapeamento de Dados
Data Mapping**

Por que dados pessoais são processados?
Why is personal data processed?

Quais dados pessoais são processados?
What personal data processed?

Os dados pessoais podem ser usados pelos seguintes motivos:
Personal data may be used for the following reasons:

Liste as razões pelas quais os dados pessoais são processados:
List the reasons why personal data is processed:

Quando são processados os dados pessoais?
When is personal data processed?

Quem – cujos dados pessoais são processados?
Who – whose personal data is processed?

Os dados pessoais podem ser processados para os seguintes titulares de dados:
Personal data may be processed for the following data subjects:

3.2 Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 1 de 8 / Page 1 of 8
		Data / Date:

PLT-USC-0001	REVISÃO / REVISION
---------------------	---------------------------

Este document deve ser usado para conduzir uma avaliação de impacto da proteção de dados na Braille Biomédica.
 This document is to be used to conduct a data protection impact assessment at Braille Biomédica.

Passo 1 – Determinando a necessidade / Step 1 – Determining the need

O processo envolve algum dos seguintes: Does the process involve any of the following:	Sim/Yes	Não/No
A coleta, uso ou compartilhamento de informações de saúde dos titulares de dados existentes? The collection, use or sharing of existing data subjects' health information?		
O uso de informações de saúde existentes para um novo propósito? The use of existing health information for a new purpose?		
O compartilhamento de informações de saúde dos titulares de dados entre organizações? The sharing of data subjects' health information between organisations?		
A vinculação ou correspondência de informações de saúde dos titulares dos dados que já são mantidas? The linking or matching of data subjects' health information that is already held?		
A criação de uma base de dados ou registo que contenha informação sobre a saúde dos titulares dos dados? The creation of a database or register which contains data subjects' health information?		
O compartilhamento de informações de saúde dos titulares de dados para fins de pesquisa ou estudos (independentemente de as informações serem anônimas)? The sharing of data subjects' health information for the purpose of research or studies (regardless of whether the information is anonymised)?		
A introdução de novas políticas e protocolos de prática relativos ao uso de informações pessoais dos titulares de dados? The introduction of new practice policies and protocols relating to the use of data subjects' personal information?		
A introdução de novas tecnologias em relação ao uso de informações pessoais dos titulares de dados, ou seja, novos sistemas de TI, linhas telefônicas, acesso online, etc? The introduction of new technology in relation to the use of data subjects' personal information, i.e., new IT systems, phone lines, online access, etc?		
Algum outro processo envolvendo informações de saúde dos titulares de dados que apresente risco aos seus "direitos e liberdades"? Any other process involving data subjects' health information that presents a risk to their "rights and freedoms"?		

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 2 de 8 / Page 2 of 8
		Data / Date:

PLT-USC-0001	REVISÃO / REVISION
---------------------	---------------------------

Se a resposta for sim para uma ou mais das perguntas acima, é necessária uma avaliação de impacto da proteção de dados. Prossiga para a Etapa 2.
 If the answer is yes to one or more of the above questions, a data protection impact assessment is required. Proceed to Step 2.

Passo 2 – Avaliando os riscos / Step 2 – Assessing the risks

Recolha de informação – Os dados pessoais devem ser tratados de forma lícita, justa e transparente em relação ao titular
Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the subject

Quais informações estão sendo coletadas e como?
 What information is being collected and how?

De onde as informações estão sendo coletadas e por quê?
 Where is the information being collected from and why?

Com que frequência as informações são coletadas?
 How often is the information being collected?

Uso da informação – Os dados são obtidos para fins específicos, explícitos e legítimos?
Information use – Is the data obtained for specified, explicit and legitimate purposes?

Qual é o propósito de usar as informações?
 What is the purpose of using the information?

Quando e como as informações serão processadas?
 When and how will the information be processed?

3.2 Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 3 de 8 / Page 3 of 8
		Data / Date:
PLT-USC-0001	REVISÃO / REVISION	

O uso das informações está ligado ao(s) motivo(s) para as informações serem coletadas?
 Is the use of the information linked to the reason(s) for the information being collected?

Atributos de informação – Os dados pessoais devem ser precisos e, quando necessário, mantidos atualizados
Information attributes – Personal data shall be accurate and, where necessary, kept up to date

Qual é o processo para garantir a precisão dos dados?
 What is the process for ensuring the accuracy of data?

Quais são as consequências se os dados forem imprecisos?
 What are the consequences if data is inaccurate?

Como os processos garantirão que apenas os dados existentes sejam divulgados?
 How will processes ensure that only extant data will be disclosed?

Segurança da informação – Os dados pessoais devem ser processados de forma a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas
Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Quais controles estão em vigor para proteger apenas o acesso autorizado aos dados?
 What controls are in place to safeguard only authorised access to the data?

Como os dados são transferidos; o processo é seguro e eficaz?
 How is data transferred; is the process safe and effective?

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 4 de 8 / Page 4 of 8
		Data / Date:
PLT-USC-0001	REVISÃO / REVISION	

Acesso do titular dos dados – Os dados pessoais devem ser precisos e, quando necessário, mantidos atualizados
Data subject access – Personal data shall be accurate and, where necessary, kept up to date

Quais processos estão em vigor para o acesso do titular dos dados?
 What processes are in place for data subject access?

Como podem os titulares dos dados verificar a licitude do tratamento dos dados sobre eles detidos?
 How can data subjects verify the lawfulness of the processing of data held about them?


Como os titulares dos dados solicitam que as imprecisões sejam corrigidas?
 How do data subjects request that inaccuracies are rectified?

Divulgação de informações – Os dados pessoais devem ser processados de maneira a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas
Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

As informações serão compartilhadas fora da organização; os titulares dos dados estão cientes disso?
 Will information be shared outside the organisation; are data subjects made aware of this?

Por que essas informações serão compartilhadas? Isso é explicado aos titulares dos dados?
 Why will this information be shared? Is this explained to data subjects?

Existem procedimentos robustos para solicitações de terceiros que impedem o acesso não autorizado?
 Are there robust procedures in place for third party requests which prevent unauthorised access?

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 32 de 33 / Page 32 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

3.2 Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 5 de 8 / Page 5 of 8
		Data / Date:

PLT-USC-0001	REVISÃO / REVISION
--------------	--------------------

Retenção de dados – Os dados pessoais devem ser mantidos de uma forma que permita a identificação dos titulares dos dados por não mais do que o necessário para os fins para os quais os dados pessoais são processados
Retention of data – Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

Quais são os períodos de retenção associados aos dados?
 What are the retention periods associated with the data?

Qual é o processo de descarte e como isso é feito de forma segura?
 What is the disposal process and how is this done in a secure manner?

Se os dados forem movidos para fora do local, qual é o processo; como garantir a segurança dos dados?
 Where is data stored? If data is moved off-site, what is the process; how can data security be assured?

Passo 3 – Mitigação do risco / Step 3 – Risk mitigation

Coleta de informações – O risco Information collection – The risk

Os dados pessoais são coletados sem motivo ou propósito – risco aumentado de divulgação.
 Personal data is collected without reason or purpose – increased risk of disclosure.

Coleta de informações – A mitigação Information collection – The mitigation

As razões para a coleta de dados devem ser claramente indicadas e todo o pessoal deve entender por que os dados foram coletados.
 The reasons for data collection must be clearly stated and all personnel must understand why the data has been collected.

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 6 de 8 / Page 6 of 8
		Data / Date:

PLT-USC-0001	REVISÃO / REVISION
--------------	--------------------

Uso da informação – O risco Information use – The risk

Os dados pessoais são usados por motivos não explicados ou esperados pelos titulares dos dados.
 Personal data is used for reasons not explained to, or expected by, the data subjects.

Uso da informação – A mitigação Information use – The mitigation


Explique e exiba claramente aos titulares dos dados como suas informações serão usadas. O compartilhamento de dados requer uma ação positiva, ou seja, opt-in, não opt-out.
 Clearly explain and display to data subjects how their information will be used. Data-sharing requires a positive action, i.e., opting in, not opting out.

Atributos de informação – O risco Information attributes – The risk

Os dados são imprecisos ou não estão relacionados ao titular dos dados.
 Data is inaccurate or not related to the data subject.

Atributos de informação – A mitigação Information attributes – The mitigation

Certifique-se de que procedimentos robustos estejam em vigor para garantir que os dados mantidos sobre os titulares dos dados sejam precisos, atualizados e reflitam os requisitos do titular dos dados para o qual foram destinados.
 Make sure robust procedures are in place to ensure the data held about data subjects is accurate, up to date and reflects the requirements of the data subject for which it was intended.

	PLT-USC-0001 Política Geral de Proteção de Dados / General Data Protection Regulation Policy	Pág. 33 de 33 / Page 33 of 33
		Vig. / Eff. 15/03/2024
		Revisão / Revision 01

3.2 Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 7 de 8 / Page 7 of 8
		Data / Date:

PLT-USC-0001	REVISÃO / REVISION
---------------------	---------------------------

**Segurança da informação – O risco
 Information security – The risk**

Acesso não autorizado a dados devido à falta de controles eficazes ou falhas de segurança/procedimento.
 Unauthorised access to data due to a lack of effective controls or lapses of security/procedure.

**Segurança da informação – A mitigação
 Information security – The mitigation**

Garantir que a equipe esteja ciente da necessidade de aderir aos protocolos e políticas de segurança da organização; realizar treinamento para aprimorar os controles atuais.
 Ensure that staff are aware of the requirement to adhere to the organisation's security protocols and policies; conduct training to enhance current controls.

**Acesso do titular dos dados - O risco
 Data subject access – The risk**

Os titulares dos dados não podem acessar as informações mantidas sobre eles ou determinar se estão sendo processadas legalmente.
 Data subjects are unable to access information held about them or to determine if it is being processed lawfully.

**Acesso do titular dos dados - A mitigação
 Data subject access – The mitigation**

Garantir que os titulares dos dados estejam cientes do acesso aos serviços online e conheçam o procedimento para solicitar que as informações mantidas sejam alteradas para corrigir eventuais imprecisões.
 Ensure that data subjects are aware of access to online services and know the procedure to request that information held be amended to correct any inaccuracies.

	Anexo B – Avaliação de impacto da proteção de dados / Annex B – Data protection impact assessment	Pág. 8 de 8 / Page 8 of 8
		Data / Date:

PLT-USC-0001	REVISÃO / REVISION
---------------------	---------------------------

**Divulgação de informações - O risco
 Information disclosure – The risk**

A redação de informações antes da divulgação pode não impedir que os titulares dos dados sejam identificados – ou seja, a referência ao titular dos dados pode ser feita nos detalhes de uma consulta ou carta de referência.
 Redacting information before disclosure might not prevent data subjects being identified – i.e., reference to the data subject may be made within the details of a consultation or referral letter.

**Divulgação de informações - A mitigação
 Information disclosure – The mitigation**

Certifique-se de que a política de divulgação seja robusta o suficiente para garantir que as informações de identificação sejam removidas.
 Make sure the policy for disclosure is robust enough to ensure that identifying information is removed.

**Retenção de dados - O risco
 Retention of data – The risk**

Os dados são retidos por mais tempo do que o necessário ou o processo de descarte correto não é seguido.
 Data is retained longer than required or the correct disposal process is not adhered to.

**Retenção de dados - A mitigação
 Retention of data – The mitigation**

Certifique-se de que as políticas e protocolos de prática estipulem claramente os períodos de retenção de dados e os processos de descarte. Revise e atualize protocolos e políticas e, se necessário, forneça treinamento para a equipe para garantir a conformidade.
 Ensure that practice policies and protocols clearly stipulate data retention periods and disposal processes. Review and update protocols and policies and, if necessary, provide training for staff to ensure compliance.