b/luz

GUIDE

ANONYMIZATION AND PSEUDONYMIZATION

The Brazilian National Data Protection Authority (ANPD) has opened a public consultation on the draft ***Anonymization and Pseudonymization Guide for the Protection of Personal Data.***

The objective is to hear from society regarding the guide, clarify doubts, and receive contributions. The consultation will be available on the Participa+Brasil platform for the next days, and all contributions must be submitted by **February 28th.**

WHAT DOES ANPD UNDERSTAND AS ANONYMIZATION PROCESS?

Anonymization is the process by which data loses the possibility of direct or indirect association with an individual, thus becoming anonymized.

Anonymized data is data that was initially linked to a natural person but has subsequently undergone a process of anonymization. Due to the removal of **direct and indirect identifiers**, these data lose, in principle, their personal character.

Direct identifier is the data that by itself allows to uniquely identify a natural person, without the need to combine it with data from other sources. The typical direct identifier of a data subject is their full name or their ID number.

The **indirect identifier,** on the other hand, is considered the data that by itself does not have the ability to identify someone, but can be aggregated and linked to auxiliary data to identify a natural person, such as age and residence ZIP code.

Examples of Anonymization Techniques

Applicable techniques in the dataset to, in principle, eliminate the possibility of identification

ADDING NOISE
Make small modifications to the original data by adding noise

GENERALIZATION
Group data with common characteristics at a higher level of granularity

MASKING
Partially hide the information, eliminating the possibility of identification

PERMUTATION
Reorganize the values of the data within a set of information

SUPPRESSION
Delete records or part of them from a structured set of information

BLUR OR PIXELIZATION
Blur or reduce the resolution of an image or area of interest

Anonymized data is not considered personal data and, therefore, is not subject to the protection of LGPD, unless the anonymization process to which it has been subjected is reversed by some effective means.

ANONYMIZATION DOES NOT COMPLETELY ELIMINATE THE RISK OF DATA REIDENTIFICATION

The preliminary study emphasizes that anonymization does not guarantee a reduction of the probability of data identification to zero. Considering the huge volume of publicly available auxiliary data and the development of new data processing technologies, even after the anonymization process there is a **reidentification risk**.

In order to be considered effective, the anonymization process must not be reversible:

1. **solely by means of the data controller or;**
2. **through reasonable efforts.**

To analyze the possibilities of reversal, the preliminary study interprets two important concepts:

REASONABLE EFFORTS
WHAT CAN WE CONSIDER REASONABLE EFFORTS?

OWN MEANS
WHAT CAN WE CONSIDER OWN MEANS?

- Companies have the duty to manage the risk of re-identification of data subjects, for example, by using known methodologies (k-anonymization, t-closeness, l-diversity), to ensure that the anonymization process persists over time.
- To determine the level of data anonymization, the degree of usefulness of the information in relation to the applied procedure must be considered.

INSIGHTS: ANONYMIZATION AND THE PRINCIPLES OF LGPD

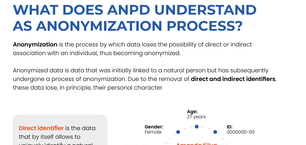
1 Application of the LGPD
Anonymization begins with personal data processing operation. Therefore, the initial phase of the anonymization process, in which personal data is still associated with a natural person, is regulated by LGPD.

2 Adequacy and purpose
Anonymization is not able to regularize an initially illicit activity. If the initial processing did not have a legitimate legal basis, for example, the anonymization process is not able to remedy this defect.

3 Transparency
Controllers must inform data subjects that personal data will be anonymized. In case of secondary use of personal data, the controller must do so in a manner compatible with the purposes initially informed to the data subjects.

WHAT DOES ANPD UNDERSTAND AS PSEUDONYMIZATION?

According to the preliminary study, pseudonymization of personal data involves replacing any identifiable characteristics of the data with a pseudonym, i.e., a value that does not allow for the direct identification of the data subject.



In the example, the data cannot be assigned to Amanda Silva unless additional information about the pseudonymization secret is provided.

Amanda Silva = 000X1

In order for pseudonymization to occur, the secret must:

- be kept in a separate database from the pseudonymized data;
- be subject to technical and organizational measures that ensure that personal data cannot be linked to an individual

Pseudonymization Techniques

applicable to the dataset to reduce the possibility of identification

REPLACEMENT
Replace data with pseudonyms or codes

OBFUSCATION
Transform data in a way that makes it harder to identify a person

TOKENIZATION
Replace data with tokens or codes that have no meaning outside the context of the system

ENCRYPTION
Convert data into an encrypted format that can only be decrypted with a key

MASKING
Hide information partially, reducing the possibility of identification

SALTING
Add a random value to the data before encryption

Is Cryptography anonymization?

As a rule, according to the ANPD, no. Since the original information needs to be accessible, the encryption process is designed to be reversible. However, the authority acknowledges that, in some circumstances, cryptographic algorithms (symmetric, asymmetric, and hash) that perform one-way processing can meet the requirements for data anonymization.

Pseudonymization methodology

In the preliminary study, the ANPD states that it is essential for companies to develop a data pseudonymization methodology if they apply this procedure. This methodology, according to the Authority, involves several stages, including the development of policies and procedures, key and algorithm protection, monitoring, training, and documentation.

Here at b/luz, we are already preparing our contribution

All information in this infographic is based on provisional understandings from ANPD detailed in the **Guide to Anonymization and Pseudonymization for the Protection of Personal Data**. These understandings are subject to public consultation and, here at b/luz, we are already preparing our contribution.

You can contribute to the public consultation directly through the Participa+Brasil Platform or contact us at **fernando@baptistaluz.com.br** so that we can represent your interests.