TEMPLATE FOR SUBMITTING CONTRIBUTIONS FOR PUBLIC CONSULTATION NO. 2/2021*

NAME OF INSTITUTION/INDIVIDUAL:

CPF/CNPJ:

BRAZILIAN DATA PROTECTION AUTHORITY (ANPD)

INTRODUCTION

The following questions seek to guide the public consultation for new ANPD and data subject notification regulations related to security incidents that may result in risks or relevant damage. Although the law establishes certain minimum criteria, the ANPD must regulate aspects such as the notification timeframe, the definition of the notification form and the best way to submit the information, in accordance with Article 48 (and those following it) of Law No. 13,709/2018 – the Brazilian Data Protection Law (LGPD) – along with item 3 of the ANPD's 2021-2022 Regulatory Agenda.

Topics that are presented in this document include ANPD assessment criteria for relevant risk or damage, the distinction between risk and damage, relevant considerations for assessing risk or damage, information that data controllers must submit to the ANPD and data subjects, reasonable timeframe for notifying both the ANPD and data subjects, as well as possible exceptions to this notification.

Other topics considered relevant for analyzing the impact of regulations may also be inserted in the table below.

INCOMING CONTRIBUTIONS

IMPORTANT: Comments and suggestions regarding this public consultation should be substantiated and justified. If international experience is cited, please insert the corresponding electronic address.

TOPIC/QUESTION	CONTRIBUTION/INSTITUTION
When can an incident lead to relevant risks or damage for the data subject? What criteria should the ANPD consider in assessing risks or damage as relevant?	
Should relevant risks or damage be subdivided into further categories (e.g. low, medium, high, etc.)? How should these categories be distinguished? Should low-level risks or damage be considered relevant or irrelevant?	
How should risks to the data subject be distinguished from damage? How are these concepts related?	
What should be considered during incident risk assessment?	
What information must data controllers notify the ANPD about, in addition to those already listed in §1º of Article 48?	
What would be a reasonable timeframe for data controllers to inform the ANPD about a given security incident? (Article 48, §1º)	
What would be a reasonable timeframe for data controllers to inform data subjects of a given security incident? (Article 48, §1°) What information should this notification contain? Should it differ from what is stated in Article 48 §1°?	

What is the most appropriate way to communicate an incident to data subjects? Should communication always be direct and individualized (by post, e-mail, etc.) or, in certain circumstances, should public forms of communication be allowed (press releases, internet publications, etc.)?	
In which situations should there be an exception to notifying the ANPD?	
In which situations should there be an exception to notifying data subjects?	
What possible criteria should be adopted by the ANPD when analyzing the severity of a security incident? (Article 48, §2°)	
Is there a recommended methodology for analyzing the severity of a security incident? If so, which one(s)?	
What measures, whether technical or administrative, should the ANPD determine data controllers take after the security incident is reported?	
SUGGESTION OF REGULATION (IF ANY)	
Article. Xxxx	
Article. Xxxx	

**This document is a translation by Mattos Filho for understanding purposes only. Click here to access the original form.*