Art. 4º O controlador deverá comunicar à ANPD e ao titular os incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante aos titulares.	Sugestão de redação: Art. 4º O controlador deverá comunicar à ANPD e, se for o caso, aos titulares, os incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante. § 1º - A comunicação ao titular de dados afetado deve ocorrer exclusivamente: I - caso seja verificado alto risco aos direitos e liberdades dos titulares envolvidos; II - a partir da ciência do controlador de que existem medidas assecuratórias a serem implementadas pelo titular afetado para efetivamente mitigar ou reduzir os riscos ou danos relevantes identificados; ou III - a partir da determinação pela ANPD, após iniciado processo de comunicação de incidente de segurança com dados pessoais, visto a constatação pela Autoridade de que existem medidas assecuratórias a serem implementadas pelo titular afetado para efetivamente mitigar ou reduzir os riscos ou danos relevantes identificados. § 2º - Não será necessário comunicar à ANPD e aos titulares a respeito de um incidente de segurança com dados pessoais nas seguintes hipóteses: a) caso o controlador tenha implementado medidas adicionais suficientes para mitigação ou reversão dos riscos ou danos relevantes identificados; b) caso os dados afetados sejam ininteligíveis; c) caso o incidente seja causado pelo próprio titular; d) caso os dados envolvidos no incidente sejam previamente públicos e o incidente não altere a disponibilidade e publicidade desses dados pessoais; e) em caso de culpa exclusiva do titular ou de terceiro. § 3º - Em caso de controladoria conjunta, será responsável pela comunicação o controlador que tiver dado causa ao incidente de segurança com dados pessoais. Justificativa: É importante que a obrigação de notificar a ANPD seja desassociada da obrigação de notificar os titulares de dados pessoais. Tal dissociação já ocorre, por exemplo, dentro da estrutura normativa da GDPR, que em seus arts. 33 e 34 disciplina, respectivamente, (i) a notificação à autoridade em caso de incidente de segurança com dados pessoais que acarrete risco aos direitos e liberdade dos titulares; e (ii) a comunicação aos titulares nos casos de alto risco aos direitos e liberdades dos titulares envolvidos. Como se vê, não há gatilhos idênticos que justifiquem o envolvimento de ambos ao mesmo tempo e isso ocorre, naturalmente, porque o propósito da notificação para cada um é diferente. Até mesmo o EDPB, em suas Diretrizes 9/2022 sobre a notificação da violação de dados pessoais sob o GDPR, reafirma que “o principal objetivo da notificação aos indivíduos é fornecer

	informação específica sobre as medidas que devem adotar para se protegerem (...) a comunicação ajudará as pessoas a adotarem medidas para se protegerem de quaisquer consequências negativas da violação". Para fins ilustrativos, o procedimento de notificação estabelecido pela SENACON em casos de recall é de que primeiro se notifica à SENACON sobre o início das investigações em caso de possibilidade de produtos ou serviços nocivos ou periculosos colocados no mercado e somente se concluída ou identificada a nocividade ou periculosidade é que surge o dever de informar os consumidores por meio de aviso de risco de acidente ao consumidor. Ainda que resguardadas as devidas diferenças regulatórias com a presente minuta de Regulamento, o que se busca destacar é que os gatilhos para notificar cada um (SENACON e consumidor) não são os mesmos (Portaria nº 618/2019) e que se tal postura pode ser adotada em casos nos quais a apuração envolve possíveis riscos à própria vida dos consumidores, não há por que regulamentar a questão de forma diversa aqui. Em relação à comunicação aos titulares de dados pessoais, em linha com o relatado no AIR (fl. 20), um dos principais benefícios/finalidades da comunicação aos titulares de dados é o de fornecer a informação para que ele possa adotar, caso queira, as medidas assecuratórias cabíveis para reduzir o risco do incidente. Por conta disso, nem todo incidente reportável à ANPD deveria atrair - de forma obrigatória - a notificação ao titular. Essa notificação deveria ocorrer mediante gatilho da existência e identificação de que há medidas assecuratórias a serem implementadas pelo titular que podem ajudá-lo na mitigação e redução dos riscos ou danos. Assim, esse dever de comunicação aos titulares de dados não deve ser confundido com as características próprias da publicização da sanção (art. 52, IV, LGPD) e deveria ser atrelado à finalidade efetiva a que se presta a comunicação ao titular: a possibilidade de implementação, pelo titular, de medidas mitigadoras e assecuratórias cabíveis àquela situação. Nestes casos, situações em que não haja medidas assecuratórias que possibilitem uma ação positiva por parte do titular devem ser excluídas do dever de comunicação aos titulares de dados. Além disso, sugere-se a inclusão (i) de um parágrafo que explicite as hipóteses em que não é necessário comunicar um incidente de segurança à ANPD e aos titulares e (ii) de um parágrafo que determine

	parâmetros para a comunicação do incidente de segurança em caso de controladoria conjunta, tendo em vista que a minuta se omitiu a respeito do assunto.