Célian Hirsch | 27.05.2024

Devoir d'annonce des cyberattaques

	FINMA	PFPDT	OFCS
Conditions	La cyberattaque vise des actifs d'importance critique et met en danger un ou plusieurs éléments faisant l'objet d'une protection (objectifs de protection) dans les fonctions d'importance critique et leurs processus.	La cyberattaque constitue une violation de la sécurité des données et entraîne vraisemblablement un risque élevé pour les personnes concernées.	La cyberattaque: -met en péril le fonctionnement de l'infrastructure critique concernée; -a entraîné une manipulation ou une fuite d'informations; -n'a pas été détectée pendant une période prolongée, en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques, ou -s'accompagne d'actes de chantage, de menaces ou de contrainte.
Délai	Annonce dans les 24 heures, puis annonce détaillée dans les 72 heures	Dans les meilleurs délais	Dans les 24 heures
Contenu	L'annonce doit contenir la nature de la cyberattaque, ses conséquences et les mesures prises ou envisagées (cf. les sources ci-dessous pour les différences selon l'autorité destinataire).		
Sources juridiques	Art. 29 al. 2 LFINMA Communication FINMA sur la surveillance 05/2020 Cf. ég. Circulaire 2023/1 sur les risques et résilience opérationnels	Art. 5 let. h LPD Art. 24 LPD Art. 15 OPDo	Art. 74*d* s. LSI Art. 18 p-OCyS

Cf. ég. HIRSCH CÉLIAN, Le devoir d'informer lors d'une violation de la sécurité des données, Avec un regard particulier sur les données bancaires, thèse, Genève 2023