FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE SÉCURITÉ FOURNISSEUR DE SERVICE NUMERIQUE

(Article 20 du décret n° 2018-384 du 23 mai 2018)

Ce formulaire doit être complété et transmis par le fournisseur de service numérique (FSN), de préférence par voie électronique et chiffré, à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) selon les modalités précisées sur son site internet (www.ssi.gouv.fr). Il peut également être transmis à l'ANSSI par voie postale à l'adresse suivante : Agence nationale de la sécurité des systèmes d'information, 51, boulevard de La Tour-Maubourg, 75700 Paris 07 SP.

1. Informations générales

Date de la déclaration : *(jj/mm/aaaa)*

Dénomination du FSN :

Type de FSN : Place de marché en ligne
Moteur de recherche en ligne
Service d'informatique en nuage

Le cas échéant, référence de l'incident propre au FSN :

Le cas échéant, référence de l'incident fournie par l'ANSSI :

2. Informations sur le déclarant

Le déclarant est la personne chargée au nom du FSN d'effectuer la présente déclaration. Lorsque le FSN est établi hors de l'Union européenne, le déclarant est le représentant du FSN sur le territoire national conformément aux dispositions prévues à l'article 16 du décret n° 2018-384 du 23 mai 2018.

Nom :

Prénom :

Service :

Fonction :

Adresse postale :

Téléphone :

Adresse(s) électronique(s) :

3. Informations sur le ou les points de contact

Le ou les points de contact sont les personnes chez le FSN auprès desquelles l'ANSSI peut obtenir (si possible 24 heures/24 et 7 jours/7) des informations complémentaires relatives à l'incident.

Le déclarant est-il le point de contact ?

Sinon, coordonnées du ou des points de contact :

	Contact 1	(Contact 2)	(Contact 3)
Nom(s) :			
Prénom(s) :			
Service(s) :			
Fonction(s) :			
Adresse(s) postale(s) :			
Téléphone(s) :			
Adresse(s) électronique(s) :			

4. Description de l'incident sur le réseau et système d'information

Dénomination du réseau et système d'information affecté par l'incident :

Description de ce réseau et système d'information :

Si ce réseau et système d'information est exploité par un tiers, nom de ce tiers :

Localisation physique de ce réseau et système d'information ainsi que des équipements de ce réseau et système concernés par l'incident :

Date et heure (heure de Paris) à laquelle l'incident a été constaté : *(jj/mm/aaaa)* Heure :

Date et heure (heure de Paris) estimées du début de l'incident : *(jj/mm/aaaa)* Heure :

Description générale de l'incident :

Description de l'atteinte à la sécurité de ce réseau et système d'information :

Description du ou des services numériques, dépendant de ce réseau et système d'information, qui sont affectés par l'incident :

5. Impacts de l'incident sur le ou les services numériques affectés

Les impacts sont à considérer en prenant en compte les paramètres précisés à l'article 3 du règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018.

Nombre d'utilisateurs touchés par l'incident :

Méthode utilisée pour estimer ce nombre d'utilisateurs touchés par l'incident :

Durée de l'incident :

Portée géographique de l'incident :

Si l'incident affecte la fourniture du ou des services numériques dans d'autres Etats membres, liste de ces Etats membres :

Si le FSN a déclaré l'incident dans d'autres Etats membres, liste de ces Etats membres :

Description des impacts de l'incident sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données des utilisateurs et des services numériques affectés :

Description de la nature des préjudices matériels ou immatériels subis par les utilisateurs en raison de l'incident, notamment en ce qui concerne la santé, la sécurité et les dommages causés aux biens :

6. Impact significatif de l'incident

Les critères prévus à l'article 4 du règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 permettent de déterminer si l'incident a un impact significatif.

Est-ce que le ou les services numériques affectés ont été indisponibles pendant plus de 5 000 000 heures-utilisateur (une heure-utilisateur correspondant au nombre d'utilisateurs touchés dans l'Union Européenne pendant une durée d'une heure) ?

Est-ce que l'incident a entraîné, pour plus de 100 000 utilisateurs dans l'Union européenne, une perte de l'intégrité, de l'authenticité ou de la confidentialité des données stockées, transmises ou traitées ou des services affectés ?

Est-ce que l'incident a engendré des risques pour la sécurité ou la sûreté publiques ou de décès ?

Est-ce que l'incident a causé un préjudice matériel à au moins un utilisateur dans l'Union Européenne dont le montant est supérieur à 1 000 000 € ?

7. Traitement de l'incident

Qualification (analyse) de l'incident :

En cas d'incident d'origine non malveillante, description des causes de l'incident :

En cas d'incident d'origine malveillante (ou attaque), description du mode opératoire et des caractéristiques de l'attaque :

En cas d'attaque, situation actuelle de l'attaque :

S'ils ont été identifiés, marqueurs techniques de l'attaque (adresses IP, noms de domaine, adresses URL, noms de fichiers ou de codes malveillants, etc.) :

Description des mesures techniques et organisationnelles prises et envisagées par le FSN pour traiter l'incident :

Si le FSN recourt à des prestataires extérieurs pour traiter l'incident, liste de ces prestataires :

8. Divers

Si des déclarations relatives à cet incident ont été effectuées par le FSN auprès d'autres organismes, liste de ces organismes :

En particulier, si un dépôt de plainte a été effectué par le FSN, service auprès duquel la plainte est déposée :

9. Observations complémentaires