Agence fédérale des médicaments et des produits de santé

Détection, évaluation et notification de fuites de données dans le cadre de la protection des données à caractère personnel

SOP numéro : DPO/003/SOP/F (1)

Nombre total de pages : 10

Annexe(s) : 1

Cette procédure est destinée à tous les employés de l'AFMPS, aux membres du Data Breach Evaluation Board (DBEB) et à l'Administrateur général.

	Nom	Fonction	Signature
Vérifié par	Christelle Beeckmans	Chef de division – Division Qualité	
	Steven Hippe	Chef de division – Division juridique	
Approuvé par	Xavier De Cuyper	Administrateur général	
	Greet Musch	Directeur général – DG PRE	
	Hugues Malonne	Directeur général – DG POST	
	Ethel Mertens	Directeur général – DG INSP	

Date d'application : voir « Application Date » dans DMS Quality

TABLE DES MATIÈRES

Détection, évaluation et notification de fuites de données dans le cadre de la protection des données à caractère personnel

1. Champ d'application et responsabilités

Cette procédure s'applique à la détection, l'évaluation et la notification d'éventuelles fuites de données liées à des données à caractère personnel qui sont traitées sous la responsabilité de l'AFMPS, et s'adresse en premier lieu à tous les collaborateurs de l'AFMPS, vu que chacun peut détecter une éventuelle fuite de données, et a donc l'obligation de notifier en interne cette éventuelle fuite de données. D'autre part, cette procédure s'adresse également aux membres du *Data Breach Evaluation Board* (DBEB), qui sont chargés de l'évaluation des éventuelles fuites de données.

2. But de la procédure

Cette procédure commence par la définition d'une fuite de données, suivie par la manière dont celle-ci peut être signalée en interne. C'est ensuite au *Data Breach Evaluation Board* d'évaluer ces éventuelles fuites de données afin d'examiner dans quelle mesure il s'agit effectivement d'une fuite de données, si celle-ci doit être notifiée à l'autorité de protection des données, si les personnes concernées doivent être averties, et enfin afin de mettre sur pied d'éventuelles mesures visant à éviter de telles fuites de données à l'avenir.

3. Définitions et abréviations

personne concernée: personne dont les données à caractère personnel ont été traitées, et qui est potentiellement la victime d'une fuite de données.

fuite de données: violation de la sécurité de données à caractère personnel entraînant l'accès indésirable, à la perte, la destruction, l'altération ou la divulgation de ces données à caractère personnel.

DBEB: *Data Breach Evaluation Board,* Conseil d'évaluation de fuite de données
Un groupe de personnes qui sont chargées de l'évaluation d'éventuelles fuites de données.

DPA: *Data Protection Authority*, l'autorité nationale de protection des données.

DPIA: *Data Protection Impact Assessment*, une analyse approfondie d'un traitement de données à caractère personnel en ce qui concerne la conformité au GDPR, et les risques de fuites de données et leur impact potentiel pour les personnes concernées.

DPO: *Data Protection Officer,* le fonctionnaire de l'AFMPS pour la protection des données.

GDPR: *General Data Protection Regulation*, Règlement général sur la protection des données
Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

4. Généralités

4.1. Obligation de notification de fuites de données

Le GDPR oblige chaque personne qui traite des données à caractère personnel à notifier à la DPA (autorité de protection des données) des fuites de données dans les 72 heures après la détection, et dans certains cas également aux personnes concernées, en d'autres mots à ceux dont on a abusé des données à caractère personnel.

4.2. Data Breach Evaluation Board (DBEB)

Dans le cadre du processus décisionnel et afin de pouvoir procéder à une décision réfléchie, il est indiqué de travailler avec un organe de concertation qui se réunit à la suite de la constatation d'une infraction, à savoir le « *Data Breach Evaluation Board* » (DBEB).

Celui-ci se compose comme suit :

- Le DPO de l'AFMPS
- Le consultant de l'AFMPS en matière de sécurité de l'information
- Le chef de division de la division Qualité ou son délégué
- Le chef de division de la division juridique ou son délégué

Voici les tâches/compétences de ce board :

- dans le délai prévu, ouvrir une enquête sur les faits de l'/des éventuelle(s) violation(s) ;
- avoir la possibilité de s'entretenir avec chaque collaborateur et de compulser tous les documents pertinents ;
- avoir accès à tous les lieux de travail et espaces qui sont liés à la violation ;
- en concertation avec la direction quotidienne de l'AFMPS, décider d'impliquer des experts externes dans l'enquête ;
- examiner si et comment de telles violations peuvent être évitées ou prévenues à l'avenir ;
- examiner des déclarations de confidentialité signées de collaborateurs ou d'experts externes qui sont concernés par l'enquête.

5. Procédure

5.1. Détection d'éventuelles fuites de données

5.1.1. Qu'est-ce qu'une fuite de données ?

On parle d'une fuite de données en cas de violation de la sécurité des données à caractère personnel qui conduit à un accès indésirable, à la perte, la destruction, l'altération ou la divulgation de ces données à caractère personnel.

Cela comprend donc de nombreux types d'incidents très différents, qui peuvent avoir eu lieu aussi bien par accident que de manière volontaire. Cela peut aller par exemple d'un collaborateur qui perd une clé USB sur laquelle se trouvent des données à caractère personnel, ou dont le laptop a été volé, ou d'un collaborateur qui envoie accidentellement par e-mail un fichier à un mauvais destinataire, à un incident où un hacker réussit à avoir accès à une banque de données de l'Agence.

5.1.2. Notification interne d'éventuelles fuites de données

Dès qu'il y a un incident qui pourrait entraîner une fuite de données, cet incident doit être notifié en interne par le collaborateur qui détecte l'incident ou par le dirigeant de ce collaborateur. Cela se fait en complétant le « Formulaire de notification de fuite de données » (voir annexe 1) et le transmettant à DPO@afmps.be avec pour objet « notification interne de fuite de données ».

5.1.3. Enregistrement d'incidents notifiés

Le DPO enregistre les notifications reçues (y compris le moment de la réception) dans le registre des incidents. Ce registre permet un suivi de l'incident notifié.

5.2. Évaluation d'éventuelles fuites de données

5.2.1. Convocation du DBEB

Le DPO transmet la notification reçue à tous les membres du DBEB, et les invite à une concertation pour évaluer la violation notifiée. Cette évaluation devrait pouvoir être terminée dans les 48 heures après la notification interne par les membres disponibles du DBEB, pour pouvoir répondre si nécessaire à l'obligation de notifier à la DPA la fuite de données dans les 72 heures après la détection.

5.2.2. Collecte des informations supplémentaires

Si le DBEB estime que des informations supplémentaires ou une étude supplémentaire sont nécessaires pour l'exécution de ses tâches, celui-ci peut décider de charger un ou plusieurs de ses membres de rechercher/réclamer les informations manquantes, ou il peut lui-même décider de faire effectuer, sous la conduite du chef de division Qualité, une enquête par

l'équipe des auditeurs internes de l'AFMPS. Les collaborateurs et sous-traitants concernés qui sont interrogés à ce sujet doivent prioritairement y apporter leur collaboration afin de fournir au plus vite les informations demandées.

5.2.3. Confirmation de la fuite de données

En fonction des informations obtenues, le DBEB évalue dès que possible s'il est effectivement question d'une violation dans le cadre de la réglementation européenne. Si ce n'est pas le cas, la procédure se termine ici et ce résultat est enregistré par le DPO dans le registre des incidents.

S'il est effectivement question d'une fuite de données, le DBEB procède toutefois à une analyse des risques.

5.2.4. Analyse des risques

Le DBEB effectue une analyse des risques dans le but de déterminer si la violation conduira à un risque considérable de conséquences préjudiciables en ce qui concerne la protection des données à caractère personnel de la/des personne(s) concernée(s). Voici quelques critères d'évaluation possibles :

1. est-il question de perte de données à caractère personnel; cela implique que l'AFMPS ne dispose plus de ces données, parce que celles-ci ont été détruites ou ont été perdues d'une autre manière;
2. est-il question d'un traitement illicite de données à caractère personnel; on entend par là la destruction accidentelle ou illicite, la perte ou l'altération de données à caractère personnel traitées, ou l'accès non autorisé aux données à caractère personnel ou la divulgation de celles-ci;
3. est-il question d'une non-conformité ou d'une vulnérabilité dans la sécurité de l'information;
4. peut-on raisonnablement supposer que la violation de la sécurité a conduit à un traitement illicite;
5. l'incident concerne-t-il des données confidentielles ou très confidentielles (cf. Article 9 du GDPR), par exemple:
    a. données relatives à l'état de santé de la personne concernée;
    b. données relatives à la situation financière ou économique de la personne concernée;
    c. données pouvant conduire à une stigmatisation ou une exclusion de la personne concernée (idées politiques, orientation sexuelle, etc.);
    d. noms d'utilisateurs, mots de passe et autres données d'ouverture de session;
    e. données pouvant être utilisées pour la fraude à l'identité.
6. la nature et l'ampleur de la violation entraînent-elles un risque considérable de subir un préjudice, par exemple:
    a. il s'agit de nombreuses données à caractère personnel par personne et/ou de données de grands groupes de personnes concernées;

b. les données à caractère personnel concernées sont diffusées ou partagées dans des chaînes (de soins); cela signifie que les conséquences d'une perte et/ou d'une altération non autorisée de données à caractère personnel peuvent survenir dans l'ensemble de la chaîne;
c. il s'agit de données à caractère personnel de personnes vulnérables.

5.2.5. Mesures provisoires urgentes (monitoring/préventives/correctives)

À partir des informations disponibles et de l'analyse des risques effectuée, le DBEB détermine si des mesures provisoires urgentes doivent être prises. Il peut s'agir de mesures correctives ou préventives pour atténuer les conséquences de la violation, pour limiter le risque de violations semblables à l'avenir, ou de mesures visant à recueillir des informations supplémentaires concernant la violation via un monitoring supplémentaire (par exemple s'il s'agit d'une violation qui est encore en cours). Le DBEB donne les instructions nécessaires aux services concernés pour l'exécution de ces mesures urgentes, et veille à ce que celles-ci soient rapidement exécutées.

5.2.6. Obligation de notification

En fonction des informations disponibles, et de l'analyse des risques effectuée, le DBEB détermine dans quelle mesure il est nécessaire de notifier la fuite de données. Il s'agit ici des notifications éventuelles suivantes:

- notification au DPA
- notification à la/aux personne(s) concernée(s)
- notifications aux services de police en cas de soupçon d'une infraction

S'il est effectivement question d'une fuite de données, mais qu'il n'est quand même pas question d'une obligation de notification, cela doit également être motivé.

5.2.7. Rapport provisoire

Le DBEB note ses constatations, les résultats de son analyse des risques, les mesures provisoires et son avis concernant l'obligation de notification dans un "rapport provisoire", et soumet celui-ci à l'administrateur général.

5.3. Décision de l'administrateur général + rapport final

L'administrateur général décide s'il est d'accord avec les constatations et l'avis du DBEB, et si les mesures et notifications proposées doivent effectivement être mises en œuvre.

Ces décisions sont documentées par le DPO dans le « rapport final », ainsi que dans le registre des incidents.

5.4. Notification de fuites de données

5.4.1. Notification au DPA

Si une notification au DPA est requise, le DPO essayera de faire cette notification dans les 72 heures après la découverte de l'infraction.

Dans la notification, il faut au minimum décrire ou communiquer ce qui suit (conformément à l'Article 33 du GDPR):

- décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
- communiquer le nom et les coordonnées du DPO auprès duquel des informations supplémentaires peuvent être obtenues;
- décrire les conséquences probables de la violation de données à caractère personnel;
- décrire les mesures prises ou proposées par l'AFMPS pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

La notification au DPA peut également comprendre les éléments suivants:

- une demande d'avis liée à la notification ou non à la personne concernée;
- le cas échéant, si l'infraction a été ou sera notifiée à la/aux personne(s) concernée(s).

L'exécution de cette notification est documentée par le DPO dans le registre des incidents.

5.4.2. Notification aux intéressés

Si une notification aux personnes concernées est requise, le DPO (sur ordre de l'administrateur général) rédige, en concertation avec le DBEB et la division Communication, un message de notification pour la/les personne(s) concernée(s).

Cette notification comprend au moins la nature de la violation, les données de contact du DPO (adresse postale et adresse e-mail) et les mesures à prendre que l'AFMPS recommande à la/aux personne(s) concernée(s) afin de limiter les conséquences négatives de l'infraction.

La/les personne(s) concernée(s), si cela ne requiert pas d'efforts disproportionnés, est/sont informée(s) de manière individuelle. Sinon, la division Communication peut proposer un plan de communication alternatif.

L'exécution de cette notification est documentée par le DPO dans le registre des incidents.

5.4.3. Notification aux services de police

En cas de soupçon d'infractions, la division juridique prendra les mesures nécessaires pour notifier la violation au procureur du Roi compétent. La division juridique tient le DPO au courant de l'exécution de la notification, et de la suite du déroulement de cette procédure.

L'exécution de cette notification est documentée par le DPO dans le registre des incidents.

5.5. Mesures correctives

C'est au responsable interne du traitement, ou au dirigeant du domaine dans lequel les violations ont été constatées de proposer d'éventuelles mesures correctives au DBEB. Une fois que les mesures correctives concrètes ont été établies avec l'approbation du DBEB, ces mesures correctives sont notifiées à la division Qualité et la mise en œuvre de ces mesures correctives est suivie par la division Qualité tel que prévu dans FAMHP/007/SOP/F « Gestion des CAPA et des actions découlant des exercices d'amélioration continue ». Le DBEB, en tant de tel, n'est ensuite plus concerné par le suivi de ces mesures correctives, ce qui n'empêche pas que les membres individuels puissent encore être concernés par ce suivi en dehors du cadre de ce board.

Si les mesures correctives concernent un traitement pour lequel une DPIA est requise, le responsable interne du traitement doit alors entreprendre un nouveau cycle DPIA une fois que la mise en œuvre des mesures correctives est terminée. Cf. DPO/002/WIT/F « Analyse d'impact relative à la protection des données ».

5.6. Clôture de la notification

Une fois que le rapport final a été rédigé, que toutes les notifications officielles ont été effectuées, et toutes les mesures correctives ont été établies et notifiées à la division Qualité, l'incident est clos. Le rapport final et les mesures correctives sont soumis à titre informatif au Comité de direction de l'AFMPS.

La clôture de la notification est enregistrée dans le registre des incidents, et tous les documents y afférent sont archivés numériquement par le DPO pour une durée de 10 ans.

6. Références et documents connexes

- DPO/002/WIT/F : « Analyse d'impact relative à la protection des données »
- FAMHP/007/SOP/F : « Gestion des CAPA et des actions découlant des exercices d'amélioration continue »

7. Historique

Détection, évaluation et notifications de fuites de données dans le cadre de la protection des données à caractère personnel		
Rédigé par: Nicolas Vervaeck	Traduit par: Marc-Antoine Collard	
Numéro de procédure	Date d'application	Raison des modifications
DPO/003/SOP/F (1)	Voir « Application date » dans DMS Quality	Première édition