Agence fédérale des médicaments et des produits de santé

REGISTRE GDPR DES ACTIVITÉS DE TRAITEMENT

SOP numéro : DPO/001/SOP/F (1)

Nombre total de pages : 8

Annexe(s) : 2

Cette procédure s'applique à tous les responsables internes d'un traitement de données à caractère personnel de l'AFMPS. Ceux-ci ont la responsabilité de documenter le traitement dans le registre de traitement GDPR, ce qui est absolument nécessaire pour être conforme au GDPR.

	Nom	Fonction	Signature
Vérifié par	Bernard Fontaine	SPOC Qualité – Division ICT	
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

Annexes

REGISTRE GDPR DES ACTIVITÉS DE TRAITEMENT

1. Champ d'application et responsabilités

Cette procédure s'applique à tous les responsables internes d'un traitement de données à caractère personnel de l'AFMPS. Ceux-ci ont la responsabilité de documenter le traitement dans le registre de traitement GDPR, ce qui est absolument nécessaire pour être conforme au GDPR.

2. But de la procédure

Cette procédure détermine dans quels cas et de quelle manière les responsables internes d'un traitement de données à caractère personnel doivent veiller à ce que ce traitement soit documenté dans le registre de traitement GDPR.

3. Définitions et abréviations

Données à caractère personnel: toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

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 (RGPD) 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.

Personne concernée: personne dont des données à caractère personnel sont traitées.

Responsable interne du traitement: collaborateur de l'AFMPS responsable d'un traitement structurel ou régulier de données à caractère personnel.

Traitement: toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

4. Généralités

L'article 30 du GDPR (art. 30 du RÈGLEMENT (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)) impose l'obligation de documenter, dans un registre des activités de traitement, tout traitement de données à caractère personnel, dans le cadre de laquelle les éléments suivants doivent au minimum être fournis:

- des informations sur le responsable du traitement (l'AFMPS) et des informations sur le DPO
- les finalités du traitement
- les catégories des personnes concernées
- les catégories des données à caractère personnel traitées
- les catégories des destinataires auxquels nous communiquons les données à caractère personnel
- les éventuels transferts de données à caractère personnel vers un pays tiers ou une organisation internationale
- les délais de conservation
- les mesures de sécurité

Dans la pratique, on se concentrera sur des activités de traitement structurelles ou régulières: par exemple, on reprendra comme 1 traitement dans le registre toute la suite d'opérations dans le cadre de toutes les demandes d'un certain type d'autorisation, et on n'enregistrera donc certainement pas séparément dans le registre chaque demande (ou chaque opération dans chaque demande).

En plus des éléments qui sont imposés à l'art. 30 du GDPR, nous enregistrons des informations supplémentaires dans notre registre, afin que ce registre puisse servir d'outil interne pratique pour aider à répondre à d'autres obligations GDPR. Nous enregistrerons également des informations sur le responsable interne, la base juridique, l'éventuel contexte juridique, l'aperçu des applications et systèmes utilisés, l'applicabilité des droits des personnes concernées, les sous-traitants concernés avec référence au contrat concerné, si une DPIA est nécessaire pour ce traitement, et des informations sur l'applicabilité des différents droits des personnes concernées. Ces informations supplémentaires doivent par exemple permettre de pouvoir répondre dans un délai acceptable à des questions de personnes concernées, ou à des demandes pour appliquer des droits de personnes concernées.

Voir annexe DPO/001/A01/F-N « Template GDPR Register of activities » pour un aperçu complet de toutes les données qui doivent être enregistrées.

5. Procédure

5.1. Initiation

Pour des traitements nouveaux ou existants qui n'ont pas encore été documentés dans le registre GDPR des activités de traitement (le registre est disponible en interne pour consultation par tous les collaborateurs internes de l'AFMPS sur le site Privacy SharePoint), le responsable interne de ce traitement doit contacter dès que possible le DPO (par exemple par e-mail à DPO@afmps.be), afin de l'informer de ce traitement. Les nouveaux traitements doivent être documentés dans le registre avant que l'on commence à effectuer le traitement de manière effective. Cela doit donc déjà se faire pendant la phase de conception du traitement.

Le DPO fournit un accès en écriture au responsable interne pour autant que celui-ci n'ait pas encore d'accès en écriture.

5.2. Compléter le registre

5.2.1. Informations générales

Le responsable interne du traitement complète le registre et peut ici, si nécessaire, également demander des explications supplémentaires au DPO concernant les différents champs du registre.

Les informations à compléter comprennent le nom du responsable interne, les services concernés, la base juridique qui permet à l'AFMPS d'effectuer ce traitement des données personnelles avec éventuellement un renvoi correspondant à une législation pertinente, les objectifs du traitement, une description des activités de traitement, des informations sur les personnes concernées, indiquer quelles données à caractère personnel sont traitées, les systèmes et applications utilisés, les éventuelles mesures de sécurité, les informations sur les sous-traitants qui sont concernés par le traitement, d'éventuelles autres parties avec qui les données sont partagées.

5.2.2. Délais de conservation

Une attention particulière doit également être consacrée à la documentation des délais de conservation qui doivent être respectés pour les différentes catégories des données à caractère personnel traitées. S'il n'existe pas de législation qui détermine explicitement ces délais de conservation, le responsable interne doit lui-même proposer un délai de conservation raisonnable avec une motivation y afférente pour ce délai de conservation. Cette motivation doit être couplée aux objectifs du traitement. Sinon, on part du principe que les données à caractère personnel doivent être supprimées à la fin du traitement.

Il est ici également important qu'il y ait une harmonisation des délais de conservation dans le registre GDPR des activités de traitement avec les délais de conservation qui sont documentés dans le cadre de l'archivage dans les archives de l'État.

5.2.3. Screening de base DPIA

Pour chaque traitement, il faut également établir s'il est nécessaire d'effectuer une DPIA (*Data Protection Impact Assessment*) (voir également « Analyse d'impact de la protection des données », DPO/002/WIT/F). À cet effet, le responsable interne du traitement doit effectuer un screening de base avec le DPO, dans le cadre duquel le formulaire DPO/001/A02/F-N « DPIA Basic Screening form » (annexe 2) doit être complété. Ce screening se déroule comme suit :

1. On examine d'abord si le traitement correspond à un traitement dans la liste des traitements pour lesquels l'autorité de protection des données a indiqué qu'une DPIA n'est pas nécessaire. Dans le cas d'un tel accord, le screening est ici achevé avec pour résultat qu'aucune DPIA n'est nécessaire. Sinon, on passe à l'étape suivante.
2. On examine si le traitement correspond à un traitement dans la liste des traitements pour lesquels l'autorité de protection des données a indiqué qu'une DPIA est nécessaire. Dans le cas d'un tel accord, le screening est ici finalisé avec comme résultat qu'une DPIA est nécessaire. Sinon, on passe à l'étape suivante.
3. Dans cette étape, une liste de 9 critères est parcourue, qui présentent chacun un facteur de risque au niveau de la protection des données. S'il y a ici au moins 2 réponses positives, on en conclut qu'il y a un risque accru, et qu'une DPIA doit donc être effectuée.

Le résultat du screening est enregistré dans le registre GDPR des activités de traitement, et le formulaire Basic Screening complété pour ce traitement est également conservé à part dans le site Privacy SharePoint.

Si une DPIA est effectivement nécessaire, c'est au responsable interne du traitement à organiser celle-ci (voir « Analyse d'impact concernant la protection des données », DPO/002/WIT/F).

Pour les nouveaux traitements (qui n'ont pas encore été réalisés au moment où le GDPR est entré en vigueur), cette DPIA doit être effectuée avant que l'on commence à réaliser effectivement ce traitement.

5.2.4. Droits des personnes concernées

Pour chacun des droits de base des personnes concernées, il faut examiner dans quelle mesure ceux-ci s'appliquent de manière effective. Il s'agit du

- Droit à l'information
- Droit à l'accès aux données à caractère personnel
- Droit à la rectification
- Droit à l'effacement des données
- Droit à la limitation du traitement
- Droit d'opposition
- Droit d'opposition contre la prise de décision automatisée, y compris le profilage
- Droit à la portabilité des données

Pour chacun des droits qui ne s'appliquent pas, il faut motiver pourquoi ceux-ci ne s'appliquent pas.

Concernant les droits qui s'appliquent, c'est au responsable interne du traitement à veiller à ce que les demandes pour appliquer ces droits puissent être traitées dans un délai raisonnable (de préférence en moins d'un mois). Cela doit donc être documenté un minimum dans le registre. C'est ici par exemple le but que le DPO reçoive une demande de rectification de données dans le cadre d'un traitement spécifique, qu'il peut facilement retrouver dans le registre si le droit s'applique bien, et si oui, à qui il doit par exemple transmettre cette demande pour exécution.

En ce qui concerne le droit à l'information, il faut vérifier si la personne concernée est informée sur le traitement de ses données d'une manière qui est conforme au GDPR (cela peut par exemple se faire via une déclaration de vie privée).

5.3. Mise à jour du registre

Si des modifications profondes sont apportées plus tard au traitement (par exemple une modification d'un sous-traitant, un changement dans les applications ou systèmes utilisés, etc.), ou si le traitement est supprimé, le responsable interne du traitement doit alors actualiser le registre dès que possible. Si nécessaire, un screening de base DPIA doit ici également de nouveau être effectué.

6. Références et documents connexes

- DPO/002/WIT/F: « Analyse d'impact concernant la protection des données »
- RÈGLEMENT (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Recommandation n° 06/2017 de l'autorité de protection des données relative au Registre des activités de traitement : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf
- Recommandation n° 01/2018 de l'autorité de protection des données concernant l'analyse d'impact relative à la protection des données et la consultation préalable: https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf

7. Historique

Registre GDPR des activités de traitement		
Rédigé par: Nicolas Vervaeck (N)	Traduit par: Marc-Antoine Collard (N->F)	
Numéro de procédure	Date d'application	Raison des modifications
DPO/001/SOP/F (1)	Voir « Application date » dans DMS Quality	Première édition