

Annexe 6 des BCR de Novartis

Organisation de la Protection des données au sein de Novartis

1. ORGANISATION GLOBALE PROTECTION DES DONNÉES, DIGITAL ET IA COMPLIANCE

Novartis a établi un programme de protection des données destiné à assurer la conformité au Droit applicable à la protection des données, gérer les risques liés à la protection des données, mettre en place de nouveaux modèles opérationnels, renforcer ses capacités et fonctionner de manière efficace et efficiente.

Le programme de protection des données repose sur les piliers suivants :

- **L'organisation globale Protection des données, Digital & IA Compliance (DPDAI)** sous la direction de Novartis Ethique, Risque & Conformité ;
- **La politique et les procédures de Novartis en matière de protection des données et d'IA**, y compris les BCR de Novartis ;
- **Le programme de surveillance centrale de la protection des données.**

L'organisation globale DPDAI est organisée autour du **Responsable Global DPDAI**, du **Directeur Innovation, Stratégie et Engagement DPDAI**, de **l'équipe Corporate DPDAI**, ainsi que de trois **équipes régionales DPDAI** correspondant aux principales zones géographiques d'activité, à savoir les Amériques, l'Europe et l'Asie-Pacifique, le Moyen-Orient et l'Afrique (APMA). Elle est complétée par **l'équipe Surveillance & Reporting DPDAI**, établie au sein de l'organisation Ethique, Risque & Conformité Corporate, et par **l'équipe Conseil juridique sur la protection des données**, établie au sein de l'organisation juridique.

L'organisation globale DPDAI est dirigée par **l'équipe de direction DPDAI (DPDAI LT)**, qui est présidée par le **Responsable Global DPDAI**. La DPDAI LT comprend le **Responsable Corporate DPDAI**, le **Responsable DPDAI Amériques**, le **Responsable DPDAI Région Europe**, le **Responsable DPDAI APMA** et le **Responsable Conseil juridique sur la protection des données**. La DPDAI LT élargie est composée également du Responsable DPDAI Allemagne, du Responsable DPDAI Chine, du Responsable DPDAI Japon, du Responsable DPDAI Amérique latine et Canada, et du Responsable Surveillance & Reporting DPDAI. La DPDAI LT est en charge d'établir et de mettre en œuvre les orientations stratégiques de protection des données, de fixer les priorités et de superviser le déploiement de contrôles effectifs.

Le **Responsable Global DPDAI** informe et conseille le plus haut niveau de la direction de Novartis, surveille et rend compte annuellement de la conformité aux lois et réglementations sur la protection des données au niveau mondial, et supervise le maintien et le respect du programme de protection des données du Groupe. Il rend compte au Directeur Ethique, Risque & Conformité de Novartis, qui est membre du Comité Exécutif de Novartis (ECN).

Novartis fait appel à un expert externe en matière de protection des données pour agir en tant que **Délégué à la protection des données du Groupe (GDPO)** pour les entités légales de Novartis établies dans l'Espace économique européen et au Royaume-Uni, et à un délégué à la protection des données pour la Suisse. Le GDPO est indépendant et reçoit régulièrement des mises à jour de la part de la DPDAI LT sur l'état de la mise en œuvre du programme de protection des données de Novartis. Le GDPO aide le Responsable Global DPDAI à

s'acquitter de ses responsabilités essentielles telles que décrites ci-dessus. Le GDPO ne devrait pas avoir de tâches qui pourraient entraîner des conflits d'intérêts.

Le **Directeur Innovation, Stratégie et Engagement DPDAI**, en impliquant étroitement les fonctions opérationnelles, évalue leurs perceptions et sensibilise la fonction DPDAI, dans le but d'en maximiser l'impact et de générer des recommandations aux équipes DPDAI sur la façon de mettre en œuvre des initiatives appropriées et percutantes. Il gère également toutes les initiatives globales DPDAI de communication et de sensibilisation/formation au sein de la fonction DPDAI, de Novartis Ethique, Risque & Conformité et de Novartis dans son ensemble.

Le **Responsable Corporate DPDAI** définit les normes de conformité à l'échelle du Groupe, soutient les acteurs et les fonctions opérationnelles globales pour identifier les risques liés à la protection des données et mettre en œuvre des contrôles liés à la protection des données dans l'ensemble de Novartis, fournit une assurance des risques à la direction de Novartis, conçoit des procédures globales clés de protection des données pour documenter et démontrer la conformité à toutes les lois et réglementations pertinentes en matière de protection des données dans le monde entier, dirige la gestion et la résolution des incidents de protection des données.

Les **Responsables DPDAI Amériques, Région Europe et APMA**, dans les zones géographiques dont ils sont responsables, s'assurent que le personnel soit suffisant et font preuve de leadership, de soutien et de coaching aux Responsables DPDAI nationaux. Ils sont chargés d'assurer un partenariat professionnel solide sur les questions de protection des données et d'efficacité opérationnelle dans leur région de responsabilité.

Outre les principaux marchés de l'EEE+ (Allemagne, France, Espagne, Italie, Royaume-Uni), de nombreux pays de l'EEE+ et des autres régions ont nommé à plein temps des **Responsables DPDAI pays** et/ou des **Managers Protection des données** chargés de superviser la mise en œuvre du programme de protection des données de Novartis dans les pays dont ils ont la responsabilité, en fournissant une aide aux fonctions opérationnelles et des conseils compétents sur les questions de protection des données, traiter les demandes locales et les plaintes des Personnes concernées, signaler les principaux problèmes de protection des données au Responsable DPDAI de leurs régions respectives, et assurer la formation et la sensibilisation à la protection des données au niveau local. Les **Responsables DPDAI pays** rendent compte opérationnellement au Responsable DPDAI de la région concernée.

Le **Responsable Conseil juridique sur la protection des données (DPLA)** assure la fourniture de conseils juridiques à l'équipe DPDAI sur les questions de protection des données à haut risque en dirigeant l'équipe DPLA. L'équipe DPLA, établie dans le cadre de la fonction juridique, est chargée de surveiller les législations et les développements réglementaires en matière de protection des données, de cybersécurité et d'IA à travers le monde afin d'identifier les nouvelles exigences et les étapes de mise en œuvre potentielles. L'équipe DPLA s'occupe également des aspects juridiques des incidents de données personnelles et fait partie de l'équipe de réponse aux incidents juridiques en cas d'incidents de cybersécurité.

Le **Responsable Surveillance & Reporting DPDAI** est chargé de suivre régulièrement la mise en œuvre du programme de protection des données de Novartis au sein des différentes unités organisationnelles de Novartis. Ce pour garantir la conformité aux lois et règlements applicables, ainsi qu'aux politiques, manuels et documents d'orientation pertinents de Novartis. De plus, il fournit régulièrement des rapports et des informations au Responsable Global DPDAI sur les risques et les tendances majeurs et émergents. Le Responsable Surveillance & Reporting DPDAI rend compte au Responsable Revue, Surveillance et Remédiation dans le cadre de la fonction Ethique, Risque et Conformité.

L'assistant du Responsable Global DPDAI aide la DPDAI LT et gère les tâches administratives associées, et est chargé de fournir une aide professionnelle au Responsable Global DPDAI, d'exécuter des tâches administratives complexes et de gérer le budget opérationnel du département.

2. DIRECTEUR ÉTHIQUE, RISQUE ET CONFORMITÉ DE NOVARTIS

Le **Directeur Ethique, Risque et Conformité (Chief Ethics, Risk & Compliance Officer (CERCO))** de Novartis, membre du Comité Exécutif de Novartis, supervise le Responsable Global DPDAI et le Délégué à la protection des données du Groupe. Le CERCO reçoit des mises à jour régulières sur l'avancement du programme de protection des données.

3. COMMUNICATION ET COORDINATION

La communication, la coordination et la collaboration au sein de l'organisation globale DPDAI sont pilotées par le Directeur Innovation, Stratégie et Engagement, facilitées par le site intranet DPDAI qui contient la vision de la protection des données et les priorités stratégiques, les coordonnées des partenaires DPDAI concernés, des directives, des modèles, des outils et des mises à jour significatives.

Historique des versions de l'Annexe 6

Date d'entrée en vigueur	Propriétaire	Version	CNIL
3 juillet 2012	Groupe Protection des données	1.0	3 juillet 2012
19 avril 2017	Groupe Protection des données	2.0	19 avril 2017
3 septembre 2018	Groupe Protection des données	3.0	3 septembre 2018
5 septembre 2019	Groupe Protection des données	4.0	5 septembre 2019
20 décembre 2024	Responsable Protection des données, Digital et IA Compliance Région Europe	5.0	20 décembre 2024