Grille d'évaluation du niveau de risque des sous-traitants existants

Le responsable du traitement doit faire appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes concernées (RGPD, art. 28, § 1). Ce modèle de grille d'évaluation permet, après avoir répertorié les sous-traitants existants, de les évaluer et de leur attribuer un niveau de risque.

Voir « Choisir ses sous-traitants et encadrer les relations contractuelles », page 268.

	Niveau 1 risque faible : absence d'accès aux données personnelles	Niveau 2 risque normal : accès et manipulation des données	Niveau 3 risque élevé : circonstances particulières
Accès aux données personnelles techniquement impossible	X		
Accès aux données personnelles non nécessaires à la réalisation du service	X		
Le sous-traitant dispose d'un programme de sécurité fondé sur des normes reconnues		X	
Le sous-traitant dispose d'un système de management du risque		X	
Le sous-traitant documente la sécurité de son système d'information		X	
Le sous-traitant fait évoluer continuellement son système d'information		X	
Le sous-traitant dispose d'un mécanisme de notification des violations de données		X	
Le sous-traitant effectue une anonymisation des données personnelles		X	
Existence d'un DPO *ou d'une personne en charge* de la protection des données		X	

	Niveau 1 risque faible : absence d'accès aux données personnelles	Niveau 2 risque normal : accès et manipulation des données	Niv risqu circon parti
Sensibilisation et formation des employés sur la protection des données		X	
Les transferts de données sont encadrés (décision d'adéquation, clauses contractuelles types, BCR, dérogation)		X	
Existence d'une politique de protection des données personnelles		X	
Le traitement porte sur des données « sensibles »			
Le traitement porte sur des personnes vulnérables			
Le sous-traitant prend des décisions fondées sur un traitement automatisé (notamment du profilage)			
Le traitement implique un transfert de données vers un pays n'offrant pas un régime de protection adéquat			
Le traitement nécessite la réalisation d'une analyse d'impact			
Le sous-traitant héberge des données dans un pays n'offrant pas un régime de protection adéquat			

Grille d'évaluation du niveau de risque des sous-traitants existants

Le responsable du traitement doit faire appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes concernées (RGPD, art. 28, § 1). Ce modèle de grille d'évaluation permet, après avoir répertorié les sous-traitants existants, de les évaluer et de leur attribuer un niveau de risque.

Voir « Choisir ses sous-traitants et encadrer les relations contractuelles », page 268.

	Niveau 1 risque faible : absence d'accès aux données personnelles	Niveau 2 risque normal : accès et manipulation des données	Niveau 3 risque élevé : circonstances particulières
Accès aux données personnelles techniquement impossible	X		
Accès aux données personnelles non nécessaires à la réalisation du service	X		
Le sous-traitant dispose d'un programme de sécurité fondé sur des normes reconnues		X	
Le sous-traitant dispose d'un système de management du risque		X	
Le sous-traitant documente la sécurité de son système d'information		X	
Le sous-traitant fait évoluer continuellement son système d'information		X	
Le sous-traitant dispose d'un mécanisme de notification des violations de données		X	
Le sous-traitant effectue une anonymisation des données personnelles		X	
Existence d'un DPO *ou d'une personne en charge* de la protection des données		X	
Sensibilisation et formation des employés sur la protection des données		X	
Les transferts de données sont encadrés (décision d'adéquation, clauses contractuelles types, BCR, dérogation)		X	
Existence d'une politique de protection des données personnelles		X	
Le traitement porte sur des données « sensibles »			X
Le traitement porte sur des personnes vulnérables			X
Le sous-traitant prend des décisions fondées sur un traitement automatisé (notamment du profilage)			X
Le traitement implique un transfert de données vers un pays n'offrant pas un régime de protection adéquat			X
Le traitement nécessite la réalisation d'une analyse d'impact			X
Le sous-traitant héberge des données dans un pays n'offrant pas un régime de protection adéquat			X