

LA PROTECTION DES DONNEES PERSONNELLES CONFORME AU NOUVEAU REGLEMENT EUROPEEN			
ROLE DE L'ENTREPRENEUR			Conformité
Collecte des données personnelles* (ex. nom, prénom, adresse, email, etc.)			OUI NON PARTIELLE
1	Avez vous désigné un responsable du traitement des données à caractère personnel ?		
2	Les données personnelles que vous collectez sont-elles strictement nécessaires à vos activités ?		
3	Des mesures techniques et organisationnelles ont-elles été réalisées afin de minimiser la quantité des données personnelles collectées ?		
4	Collectez vous des données personnelles sensibles ** ?		
5	Si oui, avez vous mis en place une classification des données sensibles ?		
6	Le traitement des données a-t-il un but de profilage (prise de décision uniquement fondée sur un traitement automatisé de données) ?		
7	Le consentement auprès des personnes concernées par la collecte a-t-il systématiquement été obtenu (au titre d'un contrat ou d'une obligation légale) ?		
Organiser son processus interne à la protection des données personnelles			OUI NON PARTIELLE
8	La confidentialité des données personnelles collectées et traitées est-elle assurée ?		
9	Le rôle et la responsabilité de chacun des acteurs impliqués dans la mise en œuvre du traitement des données sont-ils définis ?		
10	Conservez vous la preuve du recueil du consentement préalable la collecte des données personnelles ?		
11	Votre processus interne de traitement des données personnelles permet-il à la personne concernée de gérer les demandes de modifications ?		
12	Un registre des traitements des données personnelles collectées a-t-il été mis en œuvre ?		
13	Les failles de sécurité sont-elles automatiquement notifiées aux personnes concernées par le traitement de leurs données personnelles et aux autorités compétentes ?		
14	Avez-vous réalisé une étude d'impact de la collecte sur la vie privée des personnes concernées ?		
15	Lorsque l'étude d'impact révèle un risque important d'atteinte à la vie privée de la personne concernée, la CNIL en est-elle informée ?		
Protection informatique des données personnelles collectées			OUI NON PARTIELLE
16	Avez vous un responsable dédié à la sécurité informatique ?		
17	Avez vous mis en œuvre une politique de sécurité informatique interne ?		
18	Disposez vous d'une solution de management des identités ? Tracabilité des accès aux données personnelles ?		
19	La sauvegarde des données est-elle mise en œuvre ? Validée régulièrement ?		
20	Faites-vous procéder régulièrement à des tests d'intrusion (pen test) ?		
21	Disposez vous d'un Plan de Continuité d'activité en cas d'incident ? D'un audit des processus associés ?		
Le recours à des sous-traitants			OUI NON PARTIELLE
22	Vos sous-traitants vous ont-ils informés des nouvelles obligations concernant le traitement des données personnelles ?		
23	Les contrats vous liant avec vos sous-traitants comportent-ils des clauses rappelant ses obligations en matière de sécurité, de confidentialité et de protection des données collectées ?		
Désignation d'un délégué à la protection des données personnelles			OUI NON PARTIELLE
24	Un délégué à la protection des données personnelles (DPO) a-t-il été nommé en interne dans votre structure ?		
25	A défaut, les différents responsables internes du traitement des données personnelles sont-ils sensibilisés aux nouvelles missions relatives à la protection des données personnelles ?		
SOUS-TOTAL			
MAITRISE DES DONNEES PERSONNELLES			
Droit des personnes concernées			OUI NON PARTIELLE
26	Les personnes concernées ont-elles été clairement informées de l'usage de leurs données personnelles ?		
27	Leur avez-vous précisé la durée de conservation de leurs données ?		
28	Peuvent-elles exercer un droit d'accès à leurs données (accès, opposition, rectification) ?		
29	Peuvent-elles récupérer à leur demande concrètement leurs données dans un format lisible et structuré ?		
30	Avez-vous mis en place une procédure de transfert, à leur demande, de leurs données personnelles vers un autre responsable du traitement désigné par la personne concernée ?		
31	La personne concernée peut-elle demander l'effacement de ses données dans le cadre du droit à l'oubli ?		
Traitement des données personnelles des mineurs de moins de 16 ans			OUI NON PARTIELLE
32	Si vous collectez des données personnelles impliquant des mineurs, le consentement a-t-il été délivré par les titulaires de l'autorité parentale ?		
33	Les données personnelles transmises par le mineur peuvent-elles être supprimées facilement à sa demande ?		
Assurances			OUI NON PARTIELLE
34	Etes vous assuré en cas de réclamations liés aux données personnelles traitées ?		
35	Assurez vous vos données comme un actif de l'entreprise ?		
36	Avez vous consulté votre assureur sur le risque cyber (piratage, perte de données, e-réputation...)		
SOUS-TOTAL			
INTERNATIONAL			
37	Votre entreprise est-elle une multi-nationale ?		
38	Exportez vous des données hors UE ?		
39	Exportez vous des données dans un pays reconnu comme adéquat par la Commission Européenne (Suisse, Canada, Andorre, USA, Belize, Argentine, ...)		
40	Les flux du traitement des données sont-ils recensés dans un registre des exportations ?		

* Toute information se rapportant à une personne physique identifiée ou identifiable, 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.

** Données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions philosophiques ou religieuses ou l'appartenance syndicale, données génétiques, biométriques, concernant la santé, la vie sexuelle ou l'orientation sexuelle.

Fait à :

Date :

Nom du signataire :

Fonction :

Signature :