**QUESTIONNAIRE DE CONFORMITE RGPD**

 **Règlement Général sur la protection des données personnelles 2016/679 (RGPD)**

Afin de pouvoir traiter les données personnelles de manière licite, en conformité avec le Règlement européen 2016/679 (RGPD), les sociétés (responsable du traitement) ont l’obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées dans le but de satisfaire les exigences de sécurité requises par la norme et de respecter les droits des personnes physiques concernées par le traitement de leurs données personnelles de la part de la société.

Nous vous invitons à remplir la liste de contrôle suivante afin d'évaluer le niveau de conformité de votre entreprise.

**Comment remplir le questionnaire ?**

* Le document doit être complété avec les informations relatives à l'entreprise en fonction de l'activité exercée
* Si une question n'est pas pertinente pour l'activité exercée, répondez simplement « Non applicable » et la motivation.
* Il est conseillé d’indiquer les informations de détails dans le corps de votre réponse.

**Section A – OBLIGATIONS RGPD –**

**ORGANISATION ET MESURES DE SECURITE**

|  |  |
| --- | --- |
| **Question** | **Réponse** |
| 1  | La Société dispose-t-elle d'une Politique interne de protection des données personnelles ? | [*Si oui, indiquez également la date de la dernière mise à jour*] |

|  |  |  |
| --- | --- | --- |
| 2 | La Société a nommé un délégué à la protection des données personnelles (DPO) ?  |  |
| 3 | En cas de réponse négative à la précédente, la Société a procédé à une évaluation de la nécessité de désigner un DPO ? | [*En cas d'évaluation négative, résumer les raisons]* |
| 4 | La Société a adopté un registre des activités de traitement (article 30 du RGPD) ? |  |
| 5 | Si oui, indiquer la date de la dernière mise à jour du Registre des activités de traitement de la Société. |  |
| 6 | La société a réalisé l'évaluation d’impact sur les traitements considérés à risque élevé ? |  |
| 7 | La Société a-t-elle un modèle organisationnel de la confidentialité ? |  |
| 8 | Les personnes autorisées à traiter les données personnelles (par exemple les employés, les collaborateurs) ont-elles reçu des instructions précises et une lettre de désignation précise (article 29 du RGPD) ? |  |
| 9 | La Société a identifié et désigné les Administrateurs de Système qui interviennent sur ses systèmes informatiques et les serveurs ? |  |
| 10 | La Société a adopté une procédure pour prévenir, gérer, signaler toute fuite ou violation de données personnelles « data breach » (articles 33 et 34 RGPD) ? |  |
| 11 | La Société a adopté une procédure de gestion des demandes des personnes concernées concernant leurs droits (artt.15-21 RGPD) ? |  |
| 12 | La Société dispose d'une politique de cybersécurité, apte à garantir la sécurité des postes de travail, du réseau et des archives ? |  |
| 13 | La Société effectue des sauvegardes périodiques des données personnelles ? |  |
| 14 | La Société a un plan de formation du personnel pour les thématiques du RGPD et de sécurité ? |  |
| 15 | Tous les supports papier contenant des données personnelles sont stockés dans des lieux sûrs et/ou dans des zones surveillées ? |  |

**Section B – EVENEMENTS DU DERNIER SEMESTRE**

|  |  |
| --- | --- |
| **Question** | **Réponse** |
| 16 | La Société a subi un événement de violation de données personnelles, une perte d’ordinateur portable, une attaque informatique, un vol de clé USB ? |  |
| 17 | La Société a notifié un événement de violation de données à l'Autorité CNIL ? |  |
| 18 | La Société a reçu des demandes des personnes physiques concernant l’exercice de leurs droits ? |  |
| 19 | La Société a répondu selon les délais impartis par le RGPD ? |  |
| 20 | La Société a reçu des communications de l'Autorité CNIL ? |  |

**Définitions utiles :**

* ***«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.*
* **«*DPO*»*:*** Le DPO est un organe de contrôle indépendant, obligatoire pour certains types d'entreprises, qui vigile sur le respect du RGPD et l’application des normes nationales en matière de protection des données personnelles. Le DPO est le point de contact de la CNIL et des personnes concernées. Il doit s’assurer de la formation et sensibilisation interne et de la correcte application des principes du RGPD ;
* **«CNIL»:** l'autorité administrative indépendante instituée par la loi dite sur la vie privée qui a le pouvoir d'imposer des sanctions.
* **«registre des opérations de traitement»:** défini par l’art.30 du RGPD. Il contient les données d'identification du propriétaire et du DPO, les finalités des traitements, les catégories de personnes concernées traitées et les catégories de données qui leur sont référées, les catégories de destinataires auxquels les données sont transmises, les pays tiers vers lesquels sont transmises les données personnelles et les traitements associés, les durées de conservation relatives aux différentes catégories de données utilisées et la description générale des mesures de sécurité technico-organisationnelles. Sur demande, le registre est mis à disposition de l'Autorité afin qu'elle puisse vérifier les traitements.
* **«Data breach»: «violation de données à caractère personnel» :** une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. Par conséquent, la « violation de données personnelles » est un « accident » mais pas toujours de nature informatique. Si la violation de données risque d'avoir des effets graves sur les droits et libertés des personnes physiques concernées, elle doit être notifiée à la CNIL dans les 72 heures suivant son identification.

**Risque associé à chaque question posée :**

|  |  |  |
| --- | --- | --- |
| 1  | La Société dispose-t-elle d'une Politique interne de protection des données personnelles ? | Art. 5 (2). En cas de violation, risque d’amende administrative max 4M€. |

|  |  |  |
| --- | --- | --- |
| 2 | La Société a nommé un DPO ?  | Art. 37 RGPD. En cas de manquement, si la société est obligée risque amende max 2M€. |
| 3 | En cas de réponse négative à la précédente, la Société a procédé à une évaluation de la nécessité de désigner un DPO ? |  |
| 4 | La Société a adopté un registre des activités de traitement (article 30 du RGPD) ? | Art. 30 RGPD. En cas de violation, risque d’amende max 2 M€. |
| 5 | Si oui, indiquer la date de la dernière mise à jour du Registre des activités de traitement de la Société. |  |
| 6 | La société a réalisé l'évaluation d’impact sur les traitements considérés à risque élevé ? | Art. 32 e 35 RGPD. Risque amende max 2M€. |
| 7 | La Société a-t-elle un modèle organisationnel de la confidentialité ? | Art. 29 RGPD. Risque amende max 2 M€. |
| 8 | Les personnes autorisées à traiter les données personnelles (par exemple les employés, les collaborateurs) ont-elles reçu des instructions précises et une lettre de désignation précise (article 29 du RGPD) ? | Art. 29 RGPD. Risque amende max 2 M€. |
| 9 | La Société a identifié et désigné les Administrateurs de Système qui interviennent sur ses systèmes informatiques et serveur ? | Art. 32 RGPD. Risque amende max 2M€. |
| 10 | La Société a adopté une procédure pour prévenir, gérer, signaler toute fuite ou violation de données personnelles « data breach » (articles 33 et 34 RGPD) ? | Art 33 e 34 RGPD. Risque amende max 2 M€. |
| 11 | La Société a adopté une procédure de gestion des demandes des personnes concernées concernant leurs droits (artt.15-21 RGPD) ? | Art 15-21 RGPD. Risque amende max 4 M€. |
| 12 | La Société dispose d'une politique de cybersécurité, apte à garantir la sécurité des postes de travail, du réseau et des archives ? | Art. 32 RGPD. Risque amende max 2 M€. |
| 13 | La Société effectue des sauvegardes périodiques des données personnelles ? | Art. 32 RGPD. Risque amende max 2 M€. |
| 14 | La Société a un plan de formation du personnel pour les thématiques du RGPD et de sécurité ? | Art. 32 RGPD. Risque amende max 2 M€. |
| 15 | Tous les supports papier contenant des données personnelles sont stockés dans des lieux sûrs et/ou dans des zones surveillées ? | Art. 32 RGPD. Risque amende max 2 M€. |