Questionnaire relatif au RGPD

La majorité des questions ont pour réponses fermées : Oui tout à fait - Oui partiellement - Non pas du tout.

1/ Combien avez-vous de fichiers numériques de données sensibles différents au sein de votre structure ?
2/ Est-ce qu'une personne extérieure à votre structure peut avoir accès aux données numériques à caractère personnel de votre entreprise ?
3/ Quel est le secteur d'activité de votre structure ?
4/ Votre système d'information traite-t-il des données dites « sensibles » à caractère personnel telles que : la santé, l'ethnie, la religion, l'orientation sexuelle, les aspects socio-économiques, etc. ? Si oui, combien et lesquelles ?
5/ Quelle est la finalité d'utilisation de ces fichiers numériques relatifs aux données sensibles ?
6/ Votre système d'exploitation de la donnée vous permet-il de retracer l'identité de la personne dont la donnée est traitée ?
7/ Vos bases de données sont-elles revendues à des tiers extérieurs de votre structure ?
8/ Avez-vous établi un registre des traitements dont vous êtes responsable, co-responsable, ou sous-traitant ?
9/ Est-ce qu'il est prévu que le responsable du traitement doit prévenir la personne concernée par les données lorsqu'il veut réorienter le traitement vers une ou des nouvelles finalités, et fournir certaines informations obligatoires si elles ont changé ?
10/ Avez-vous désigné au sein de votre structure un délégué à la protection des données (Data Protection Officer : DPO en anglais) ?
11/ Le rattachement hiérarchique du délégué à la protection des données personnelles (DPO) garantit-il son indépendance (en prenant une décision sans influence extérieure) ?
12/ Avez-vous des procédures spécifiques pour les transferts de données vers des pays hors-unions européennes ?
13/ Avez-vous mis en œuvre des mesures techniques et organisationnelles appropriées aux enjeux et aux droits des personnes dont les données sont traitées dès la détermination des moyens du traitement, puis pendant le traitement (Cf. « Privacy by Design ») ?
14/ Avez-vous des documents qui indiquent les mesures internes que votre structure a prise pour la réalisation du traitement de données numériques (comme des stratégies précises, un registre des activités de traitement, des mécanismes créés en interne : méthodes de protection des données, des Binding Corporate Rules, etc.) (Cf. Principe d'« Accountability ») ?
15/ Avez-vous mis en place des procédures de contrôles sur l'exploitation de vos fichiers numériques "sensibles" ?
16/ Avez-vous réalisé un état des lieux des processus métiers traitant de vos données numériques à caractère personnel ?
17/ Avez-vous identifié les sous-traitants exploitant vos données personnelles dont vous êtes responsable ?
18/ Pouvez-vous justifier la base légale de chacun de vos traitements de fichiers numériques "sensibles" ?
19/ Est-ce qu'à chaque fois que vous traitez des données personnelles vous avez au préalable obtenu l'accord de chaque personne "propriétaire" de ces données ?
20/ Quelle est la nature de cet accord ?
21/ Sous quelles formes l'accord de la personne a-t-il été recueilli ?
22/ Est-ce-que la personne qui a donné son consentement est dans la capacité de le retirer aussi aisément qu'elle l'a donné (via une procédure et dispositif interne facile d'accès) ?
23/ Sous quelle forme les données sont-elles traitées et/ou conservées (Cf. « Privacy by Design ») ?

24/ Est-ce-que la personne concernée a la possibilité de s'opposer à un traitement ?
25/ Est-ce-que la personne (concernée par les données personnelles) a la possibilité de savoir si ses données sont traitées, et dispose des informations concernant : la finalité du traitement, les catégories (natures) de données visées, les destinataires à qui les données sont ou seront communiquées, la période de conservation des données (ou le critère de décision de cette durée), son droit de rectification et d'effacement et son droit à demander que le traitement de ses données soit restreint (limité), son droit de recours auprès de la Cnil, les sources des données lorsqu'elles n'émanent pas de la personne concernée (Cf. Droit d'accès) ?
26/ Donnez-vous la possibilité à la personne concernée par les données personnelles d'exercer son droit à la portabilité des données, en lui permettant (Cf. Droit de portabilité) : Que ses données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible ?
27/ Donnez-vous la possibilité à la personne concernée par les données personnelles d'exercer son droit à la portabilité des données, en lui permettant (Cf. Droit de portabilité) : Que ses données lui soient personnellement communiquées pour son propre usage ?
28/ Est-ce-que la personne concernée peut obtenir que des données l'identifiant soient complétées ou rectifiées, si elles sont inexactes (Cf. Droit à la rectification) ?
29/ Est-ce-que la personne concernée peut s'opposer au traitement (Cf. Droit d'opposition) ?
30/ Est-ce-que la personne concernée dispose d'un droit à l'effacement, « dans les meilleurs délais » (rapidement), de ses données à caractère personnel traitées (Cf. Droit à l'effacement, ou « Droit à l'oubli numérique ») ?
31/ Les données numériques disponibles ou mobilisables que vous utilisez font-elles l'objet d'un inventaire précis ?
32/ Si vous collectez des catégories particulières de données sensibles, avez-vous vérifié la licéité de leur collecte et de leur traitement ?
33/ Avez-vous une cartographie (par ex. Diagramme radar, Tableau de bord, etc.) exhaustive des données traitées dans votre système d'information ?
34/ Avez-vous identifié et listé les transferts de données personnelles hors Union Européenne ?
35/ Avez-vous réalisé une étude d'impact pour les traitements à risque notamment quand cela concerne les droits et les libertés des personnes (ex : données sensibles, fichiers de grande ampleur concernant des enfants, données génétiques, biométriques) ?
36/ Avez-vous une traçabilité de toutes vos données avec une vue unique permettant de consigner toutes les informations que l'on peut avoir sur une personne, même si ces données existent sur plusieurs fichiers ?
37/ Avez-vous instauré un dispositif d'accès différent à vos données numériques, en fonction du profil de l'utilisateur final et du niveau de traitement ?
38/ Avez-vous modifié vos CGU et CGV en les enrichissant de demandes de consentement ?
39/ Avez-vous défini contractuellement avec vos sous-traitants des exigences en termes de protection des données ?
40/ Effectuez-vous régulièrement des contrôles / audit de sécurité de vos sous-traitants informatiques (prestataires ou fournisseurs) ?
41/ Avez-vous mis en place des politiques et des procédures qui précisent les durées de conservation des données personnelles, la sécurité des données, la suppression des données, la notification en cas de violation des données personnelles, la validation périodique de la pertinence du dispositif en place, etc. ?
42/ Avez-vous mis en place des mécanismes permettant d'isoler les environnements (infrastructures) de production et de non production (test, recette) ?