CEJMA

BIONDO Killian

FERRIOL Ethan

Partie 1/3

Question 1 :

Les données personnelles sont toutes informations pouvant servir à identifier un individu précis.

Une **donnée personnelle directe** permettant une identification directe serait par exemple un nom ou un prénom qui nous ramène directement à un individu. (source : CNIL)

Une **donnée personnelle indirecte** est quant à elle une information qui peut être utilisée pour retrouver quelqu'un indirectement comme par exemple un numéro de téléphone ou une plaque d’immatriculation.

Source (economie.gouv.fr)

Exemple de traitements de données personnelles :

Une situation dans laquelle des données personnelles pourraient être traitées serait par exemple lors de l’inscription à un site, le traitement de cookies pouvant être utilisés pour identifier une machine précise sur différents sites internet mais aussi le stockage et traitement de données patients dans un hôpital.

Question 2 :

L’internaute doit être impérativement informé que ces données personnelles soient collectées : soit au moment de la collecte dans le cas d’une récupération directe ou dans un délai de 1 mois maximum pour une collecte indirecte.

Cela est par exemple le cas sur les sites internet qui demandent d’accepter le traitement des cookies à leurs lancement, les cookies doivent être explicitement autorisés puisqu'ils représentent une collecte automatique qui ne nécessite pas d'entrées utilisateurs. Il est bien entendu aussi obligé de demander son accord lors d’une collecte de données directe, par exemple lors du remplissage d’un formulaire sur un site web ou les termes et conditions du traitement des données demandées devront être présents sur la page.

Source (economie.gouv.fr)

Question 3 :

L’utilisateur doit être informé AVANT que les données soient collectés pour donner son accord (ou désaccord). Un exemple concret de ceci est lorsqu' un site demande d’accepter l’utilisation des cookies **et force** l’utilisateur à donner une réponse pour accéder au site.

Il est aussi important de comprendre que les entreprises, site, organisation etc… évoluent constamment, par ce fait leurs manières de traiter les données collectées et leur utilisation peuvent elles aussi changer. Dans ce cas, il est impératif pour l’entité d’informer l’utilisateur du changement des conditions d’utilisation, cela est le plus souvent fait par email. Dans le cas où l'entité ne **peut pas** contacter la personne concernée par les données personnelles, il faudra supprimer les informations collectées et demander la collecte à la prochaine visite du site.

Source : (CNIL)

Question 4 :

Selon le Règlement Général sur la Protection des Données (RGPD), en cas de demande d'un internaute, vous avez l'obligation de fournir un certain nombre d'informations :

1. Identité et coordonnées du responsable du traitement :
    - Nom de l'organisation
    - Coordonnées du responsable du traitement des données
    - Coordonnées du délégué à la protection des données
2. Catégories de données personnelles concernées :
    - Nature des données collectées (par exemple : nom, adresse, email, données bancaires, etc.)
3. Durée de conservation des données :
    - Période de conservation des données ou les critères permettant de déterminer cette durée
4. Droits des personnes concernées :
    - Droit d'accès, de rectification, d'effacement, à la limitation du traitement, d'opposition et à la portabilité des données
    - Droit de retirer le consentement à tout moment

Source : economie.gouve

DPO : Le délégué à la protection des données (DPO) est chargé de mettre en œuvre et vérifier le règlement européen au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Le DPO doit avoir plusieurs compétences :

- Connaissance approfondie de la législation en matière de protection des données (il doit connaître les lois et réglementation liées à la protection des données).
- L'expertise technique (il est doit avoir une bonne compréhension des aspects techniques de la protection des données, tels que la sécurité des systèmes informatiques).
- Bonne compétences en communication (il doit être en mesure de communiquer efficacement avec toutes les parties prenantes, y compris les employés, la direction et les autorités de contrôle).

(source : dastra)

La durée de conservation des données pour les factures clients est d’un délai de 5 ans.

Pendant ce délai, l'administration peut mener des contrôles.

(source : service-public.fr)

Question 5 :

Il y a différents droits de l’internaute :

- Droit d’information : L'internaute a le droit d'être informé sur la collecte de ses données personnelles.
- Droit d’accès : L'internaute peut demander à accéder à ses données personnelles détenues par une entreprise.
- Droit d’opposition : Les personnes ont le droit de s’opposer pour des motifs légitimes (le traitement de ses données).
- Droit de la portabilité : Les personnes ont le droit de recevoir leur données qui les concerne et qu’elles ont fournies à un responsable du traitement.

(source : CNIL)

Question 6 :

Dans certaines situations, fournir uniquement de l'information ne suffit pas. Il est indispensable de recueillir le consentement explicite des utilisateurs, notamment lorsqu'il s'agit d'envoyer des emails marketing. De plus, dans le cadre de l'utilisation de cookies, il peut également être nécessaire d'obtenir cet accord préalablement. Ces mesures garantissent que les utilisateurs restent informés et ont un contrôle sur l'usage de leurs données personnelles.

Source (economie.gouv.fr)

Question 7 :

En cas de non-respect des obligations relatives à la collecte de données personnelles, la CNIL peut imposer diverses sanctions, notamment des amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial de l'entreprise. D'autres mesures incluent aussi des rappels à l'ordre. Les sanctions dépendent de la gravité.

Sources (CNIL) (CNIL)

Partie 2/3

Question 1 :

Le traitement de données personnelles peut inclure l'utilisation de l'adresse IP pour suivre l'activité en ligne, les cookies pour enregistrer les pages visitées, ou encore des données biométriques comme les empreintes digitales ou la reconnaissance faciale pour déverrouiller un téléphone.

Question 2 :

Toute entreprise qui réalise un traitement de données (gestion de la paie, recrutement, fichier clients ou fournisseurs...) doit respecter le Règlement général sur la protection des données (RGPD).

Il s'applique à toute entreprise, quelle que soit sa taille et son secteur d'activité, dès lors qu'elle est établie sur le territoire de l'Union européenne ou que son activité cible directement des résidents européens.

Si une entreprise ou un sous-traitant situé en dehors de l'UE offre des biens ou services à des personnes dans l'UE (même gratuitement) ou surveille leur comportement (ex. analyse de l'audience d'un site web), ils sont également soumis aux obligations du RGPD.

Par exemple, une entreprise américaine qui propose des services en ligne à des clients européens devra se conformer au RGPD.

(Service-public)

Question 3 :

La phrase veut dire qu'il faut un accord clair avant de traiter les données d'une personne, et cette personne doit savoir de façon simple comment ses données seront utilisées. Cela protège mieux ses informations et garantit que tout est fait proprement.

Question 4 :

- **Droit à la portabilité des données**

Ce droit donne la possibilité à quelqu'un de récupérer ces données personnelles pour les réutiliser ailleurs par exemple.

- **Droit à l'oubli**

Ce droit donne la possibilité de demander une suppression complète des données qui vous sont associées, par exemple lorsque des photos compromettantes fuient sur quelqu'un suite à du cyber harcèlement.

- **Droit à notification**

Ce droit force les entreprises à avertir les utilisateurs que leurs données ont fuité suite à un piratage par exemple.

- **Droit à réparation du dommage matériel ou moral**

Ce droit donne la possibilité à une victime d'un préjudice liée à ces données personnelles (exemple suite à un piratage) de demander une compensation monétaire.

- **Action de groupe**

Cette règle donne le droit à un groupe de personnes de manifester ou se rassembler pour lancer des actions légales contre une entreprise qui aurait fait une erreur dans le traitement de leurs données personnelles.

Source :

mes démarches les droits pour maitriser vos données personnelles

Le droit d'accès

Le droit à l'effacement

Question 5 :

Le responsable du traitement des données doit garantir la sécurité et la confidentialité des données personnelles, conformément au RGPD.

Il doit protéger ces données contre tout risque d'accès non autorisé, de perte, de destruction. Pour cela, il doit mettre en place des mesures techniques et organisationnelles appropriées (chiffrement, contrôle d'accès, etc.) et évaluer régulièrement leur efficacité. En cas de violation de données, il doit informer l'autorité de contrôle dans un délai de 72 heures et, si nécessaire, les personnes concernées.

Ensuite, le responsable du traitement est également tenu d'informer les personnes concernées sur la collecte et l'utilisation de leurs données. Il doit communiquer des informations claires sur :

- L'identité du responsable,
- La durée de conservation,
- Les droits des personnes (accès, rectification, effacement, etc.),
- Les transferts hors de l'UE, le cas échéant.

Cette transparence vise à permettre aux individus de comprendre l'utilisation de leurs données et d'exercer leurs droits.

Question 6 :

1. Désignation

Le DPO est désigné pour garantir la conformité au RGPD. Sa nomination est obligatoire pour les organismes publics, les entreprises traitant des données sensibles. Il peut être interne ou externe et doit être choisi pour ses compétences en protection des données.

2. Rôles

Le DPO conseille et informe sur les obligations liées à la protection des données, surveille la conformité avec le RGPD, gère les droits des personnes concernées et collabore avec les autorités de contrôle (ex. CNIL). Il effectue aussi des audits pour évaluer la gestion des données.

3. Qualités et compétences

Le DPO doit avoir des compétences juridiques et techniques en protection des données, être indépendant, avoir un bon esprit d'analyse et d'excellentes capacités de communication pour sensibiliser l'organisation.

Question 7 :

Le registre des traitements est un document obligatoire qui répertorie les activités de traitement de données personnelles d’une organisation. Il sert à prouver la conformité au RGPD, facilite les contrôles et optimise la gestion des données. Ce registre contient des informations essentielles telles que : les finalités du traitement, les catégories de données, les destinataires, la durée de conservation et les mesures de sécurité mises en place.

Un modèle standard comprend des colonnes détaillant chaque traitement, les données concernées, le responsable, les bases légales, ainsi que les éventuels transferts hors de l'UE. Pour les entreprises de moins de 250 salariés, ce registre est requis uniquement si les traitements sont réguliers, sensibles ou présentent un risque pour les droits et libertés des individus.

Question 8 :

En cas de non-respect des obligations liées au traitement des données personnelles, le RGPD prévoit des sanctions administratives importantes. Les amendes peuvent s'élever jusqu'à 20 millions d’euros ou 4 % du chiffre d'affaires annuel mondial de l'entreprise, en retenant le montant le plus élevé. Les autorités de contrôle, comme la CNIL en France, peuvent aussi infliger d'autres sanctions, telles que des avertissements, des mises en demeure, ou encore des restrictions temporaires ou définitives du traitement des données. Ces mesures visent à protéger les droits des individus en matière de protection des données.