ACTIVITÉ (DÉCONNECTÉE) - LE QUIZ RGPD

SÉCURITÉ > 4.2 PROTÉGER LES DONNÉES PERSONNELLES ET LA VIE PRIVÉE

CONVIENT POUR	AGE	NIVEAU DE COMPÉTENCE	FORMAT	DROITS D'AUTEUR	LANGUE(S)
Chercheurs d'emploi, Jeunes en décrochage scolaire, Tous publics	Adolescents, Adultes, Seniors	Niveau 2	Fiche d'activité	Creative Commons (BY-SA)	Français

A travers ce quiz les participant.e.s comprendront leurs droits quant à l'utilisation de leurs données personnelles.

Objectif général	Connaissances, Compétences
Temps de préparation pour l'animateur	moins d'une 1 heure
Domaine de compétence	4 - Protection de l'identité et des données personnelles
Temps requis pour compléter l'activité (pour l'apprenant)	0 – 1 heure
Nom de l'auteur	Nothing 2hide
Matériel supplémentaire	Vidéo-projecteur (optionnel)
Ressource originellement créée	Français

DÉROULÉ

1 Intro

Début 2018, il n'y a pas si longtemps, vous avez reçu une flopée de mails vous expliquant que tel ou tel service en ligne (Google, Yahoo!, Microsoft, Facebook, etc.) allait changer ses conditions générales d'utilisation pour mieux respecter votre vie privée. Peut-être les avez vous jetés, peut-être avez vous cliqué trop vite, peut-être ne vous en souvenez vous plus, mais le RGPD, c'était entre autre ça.

RGPD (ou GDPR – General Data Protection Regulaiton – en anglais) signifie :

- Règlement
- Général
- de Protection
- des Données.

Un règlement est une loi, votée par l'Europe, qui s'applique à tous les pays membres. Tous les pays européens ont l'obligation d'appliquer un règlement. Le RGPD porte sur la gestion des données personnelles des citoyen.ne.s européen.ne.s. C'est une réglementation très favorable aux utilisateur.rice.s, probablement l'une des lois parmi les plus avancées en matière de protection des données des utilisateur.rice.s dans le monde.

Alors qu'est ce qui a changé avant et après le RGPD, comment celui-ci protège-t-il les utilisateurs ? Nous allons le découvrir au fil de ce petit Quiz.

Conseil médiation :

Vous pouvez utiliser cette activité comme un quiz de validation des acquis après avoir animé un ou plusieurs ateliers autour de la thématique des données personnelles. Vous pouvez sinon vous en servir en guide d'introduction aux données personnelles et à l'identité numérique.

Appropriez-vous ce quiz pour en faire une activité amusante ! Vous pouvez par exemple vous inspirer de célèbres jeux télévisés en mettant en concurrence plusieurs équipes, utiliser des buzzers, mettre une ambiance sonore… Soyez imaginatif.ve

Vous pouvez éventuellement afficher les questions par le biais d'un video-projecteur.

Pour en savoir plus sur les données personnelles, nous vous conseillons de vous référer à nos fiches outils dédiées.

2 Quiz

En fonction du nombre de participant.e.s, créer des équipes. L'idéal est d'avoir deux équipes de 3 ou 4 personnes. Poser les questions tour à tour à chaque équipe. À chaque bonne réponse, l'équipe qui a répondu marque un point. L'équipe gagnante est celle qui a le plus de points.

Parmi ces 4 propositions, laquelle n'est pas une donnée personnelle ?

1. La liste de vos sports préférés
2. Votre pointure de chaussure
3. Votre plat préféré
4. La distance de la Terre à la lune

Réponse 4. Une donnée personnelle correspond à toute info que se rapporte à une personne physique identifiée ou identifiable. La distance de la Terre à la lune n'est pas une donnée personnelle mais une information publique.

Quand est-ce que le RGPD est applicable ?

1. En mai 2018
2. En mai 2017
3. En mai 2020
4. En mai fais ce qu'il te plaît

Réponse : 1. Ça fait déjà 1 an et de nombreuses sanctions contre les entreprises qui ne le respectent pas ont déjà été prononcées : Google, Bouygues.

Parmi les entreprises de cette liste, lesquelles ne sont pas concernées par le RGPD ? Attention, il y a plusieurs réponses

1. Facebook qui héberge aux États Unis les données de Michel qui lui habite à Bourg en Bresse
2. La poste, une entreprise française qui héberge les courriels de Michel de Bourg en Bresse qui a

toujours une adresse en @laposte.net
3. La poste qui héberge les courriels de mon ami Michael, américain qui habite Bourg en Bresse
4. Facebook qui héberge les données de mon ami Michel qui réside à San Francisco

Réponse : 4. Le RGPD s'applique dès qu'il y a collecte et traitement de données personnelles et que celles-ci concernent une personne résidant sur le territoire de l'Union Européenne. Article 3 du RGPD

Est-ce que je peux vendre mes données personnelles au profit d'un tiers contre rémunération ?

(par exemple : vendre son historique de navigation tous les jours contre rémunération de 1 €)

1. Non
2. Oui, sous forme de bail très précaire, je pourrai retirer mon consentement à l'utilisation de mes données à tout moment
3. Oui mais uniquement sur une période de temps limitée
4. Oui, je peux même lui vendre un rein si je veux

Réponse : 2. Il est possible de vendre ses données personnelles contre rémunération si on s'appuie sur la base légale du consentement, prévue à l'article 6 du RGPD : « *Le traitement n'est licite que si […] la personne concernée a consenti au traitement de ses données à caractère personnel ».* Néanmoins, le texte ajoute immédiatement une condition supplémentaire importante, puisque que le consentement doit nécessairement être donné « *pour une ou plusieurs finalités spécifiques* » A la différence de la vente d'un bien qui implique un véritable transfert de propriété, l'entreprise qui collecterait des données personnelles contre rémunération serait donc obligée d'indiquer une ou plusieurs finalités précises de traitement qui la lierait ensuite dans le temps. Cependant cette cession de droits serait très précaire et s'assimilerait plutôt à une location à laquelle vous pourriez mettre fin à tout moment puisque le RGPD prévoit que l'individu doit pouvoir retirer son consentement à tout moment aussi simplement qu'il l'a accordé.

Est-ce que mon blog ou mon site perso est concerné par le RGPD ?

1. Non, je ne suis pas une entreprise comme Facebook, je ne suis pas concerné.e
2. Non, je ne revends pas les données de mes lecteur.rice.s, je ne suis pas concerné.e
3. Oui, uniquement les jours pairs
4. Oui, en tant qu'éditeur.rice, je recueille obligatoirement des données donc je dois en informer mes utilisateur.rice.s

Réponse : 4. En tant qu'éditeur.rice d'un site, vous recueillez forcément des données : les adresses IP, les heures de connexion, les pages visitées (c'est une obligation légale depuis la Loi pour la confiance dans l'économie numérique – LCEN) , les noms et adresses déposés dans tout formulaire, de contact ou de commentaire… À ce titre vous êtes soumis au RGPD et avez des obligations envers vos utilisateur.rice.s. Vous récupérez des données sur vos utilisateur.rice.s, vous avez le devoir de respecter le RGPD, c'est à dire de recueillir leur consentement éclairé. Vous devez donc leur signaler que vous recueillez des données, quel type de données, pour quelle finalité, si celles-ci font l'objet de traitement, si un tiers intervient dans leur traitement.

Est-ce que si j'ai un compte Twitter, Facebook, Instagram ou Snapchat, je suis concerné par le RGPD

1. Non car je ne recueille pas de données
2. Non car ce sont des services américains, mes données ne sont pas situées en Europe
3. Oui car le RGPD concerne tous les citoyens européens, quel que soit l'endroit où sont hébergées leurs données
4. Oui, mais uniquement les jours impairs

Réponse : 3. Vous êtes concerné par le RGPD car celui-ci s'applique aux données de tous les utilisateur.rice.s résidant sur le sol européen. Dans cette configuration, ce n'est pas vous qui recueillez des données mais le fournisseur de service, Twitter, Facebook ou Snapchat. Les sociétés opérant ces services ont l'obligation de permettre à leurs utilisateur.rice.s de récupérer leurs données, de recueillir leur consentement, bref de respecter le RGPD.

Le RGPD est la première loi sur la protection des données personnelles en France

1. Oui, il n'y avait rien avant
2. Non la première loi de protection des données personnelles est apparue avec l'arrivée de Facebook en France en septembre 2006
3. Non la première loi de protection des données personnelles est apparue avec l'arrivée du web, en 1993
4. Non, la première loi de protection des données personnelles est apparue l'année de la mort de Claude François, en en 1978

Réponse : 4. La France est un pays pionnier en matière de défense des données personnelles avec la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978. Elle est le résultat d'un

scandale qui s'est produit en 1974 : l'État français voulait créer un fichier unique recensant tous les citoyens par un numéro unique qui lui aurait permis d'interconnecter tous les fichiers de l'administration française. Devant le scandale provoqué par cette initiative, le projet a été enterré et la loi informatique et liberté a été votée.

Un éditeur de service en ligne peut-il négocier avec moi et me dire par exemple :

« Mon service ne respecte pas le RGPD et ne le respectera pas. Si tu veux l'utiliser, tu dois accepter que je recueille tes données et que je les traite et les revende sans t'en informer »

1. Oui, la vie est dure mais c'est comme ça
2. Oui, et je trouve même que c'est assez *fair-play* de prévenir
3. Oui mais uniquement les jours impairs
4. Non, c'est du chantage, on ne négocie pas avec les terroristes

Réponse : 4. Pour être conforme avec le RGPD, un service doit recueillir le **consentement** des utilisateur.rice.s. S'il n'y a qu'une chose à retenir de cette nouvelle législation, c'est bien ça. Les services recueillant et traitant vos données doivent le faire avec votre consentement **libre** (sans contraintes), **spécifique** (un consentement par type d'utilisation de données), **éclairé** (l'utilisateur.rice doit savoir comment ses données seront traitées et par qui et qu'ielle peut y mettre fin à tout moment) et **univoque** (pas de cases pré-cochées). Ce consentement ne doit pas être contraint, ce qui est le cas ici. Les conditions applicables au consentement sont définies aux articles 4 et 7 du RGPD. Attention, le recueil du consentement n'est qu'une des 6 bases juridiques prévues par le RGPD qui autorise le traitement de données à caractère personnel. Cependant, c'est la base juridique sur laquelle se fondent la plupart des services grands publics pour opérer le traitement de vos données. Plus d'informations sur les bases juridiques du RGPD sur le site de la CNIL.

Dans quel cas un site ou une application qui recueille vos données n'est pas obligé(e) de se soumettre au RGPD ?

1. Pour toute activité relative à la recherche de preuves d'une vie extra-terrestre
2. Pour toute activité relative à la sécurité nationale
3. Pour toute activité liée à la pratique du twirling bâton
4. Pour toute activité liée aux sports extrêmes

Réponse : 2. Le RGPD crée une exception pour toute activité ayant trait à la sécurité nationale. De ce point de vue, c'est une régression par rapport à la loi de 1978 qui elle ne prévoyait pas ce type

d’exception.

Le RGPD régule le traitement des données à caractère personnel et interdit le traitement de certaines d’entre elles. Dans la liste ci-dessous, quelles sont les données dont le traitement est interdit ?

1. Les données relatives à la consommation de nourriture (type d’aliments, etc.)
2. Les données aux déplacements géographiques
3. Les données liées à la consommation électrique (combien je consomme dans mon appartement, combien d’appareils, etc.)
4. Les données liées à l’orientation sexuelle

Réponse : 4. L’article 9.1 du RGPD précise la liste des données dont le traitement est interdit : « Le traitement des données à caractère personnel qui révèle l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l’appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d’identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l’orientation sexuelle d’une personne physique est interdit. » Il existe cependant de nombreuses exceptions : Consentement explicite de la personne concernée, traitement nécessaire en droit du travail, sécurité sociale, protection sociale, Sauvegarde des intérêts vitaux de la personne concernée, traitement nécessaire pour des motifs d’intérêt public, traitement par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, données à caractère personnel qui sont manifestement rendues publiques par la personne concernée.

Lorsqu’une entreprise ne respecte pas le RGPD, quelle est l’amende maximale que celle-ci peut se voir infliger par les autorités de régulation ?

1. 300 000 €
2. 3 millions €
3. 4% du chiffre d’affaires de l’entreprise concernée
4. 3 carambars

Réponse : 3. Pendant longtemps, les sanctions que pouvaient infliger la CNIL sont restées assez symboliques et étaient peu appliquées (300 000 euros, puis 3 millions avec loi République numérique). En indexant les sanctions sur le chiffre d’affaires, le RGPD a rendu les sanctions vraiment dissuasives. À titre d’exemple, Google a été la première entreprise à s’être vu infliger une amende pour non respect du RGPD. Celle-ci se monte à 50 millions d’euros. Selon la CNIL, « *les utilisateurs ne sont pas en mesure de comprendre l’ampleur des traitements mis en place par Google*

». Un point extrêmement fâcheux, puisque la CNIL en déduit que le consentement des internautes « *n'est pas valablement recueilli* », faute pour le géant américain d'avoir « *suffisamment éclairé* » ses client.e.s.

L'application jelachemonsmartphone.com me permet de savoir à quel point je suis accroc à mon smartphone.

Elle affiche le nombre d'heure d'utilisation de mon smartphone par jour. Lorsque je l'installe, RGPD oblige, Jelachemonsmartphone.com me demande mon consentement pour accéder au nombre d'heures de connexion et je lui donne. Est-ce que jelachemonsmartphone.com pourra transférer ces données à un constructeur pour que celui-ci puisse obtenir des statistiques d'utilisation de ses futurs usagers ?

1. oui, c'est même plutôt bien que les constructeurs puissent avoir ces infos, en plus j'ai déjà donné la permission à jelachemonsmartphone.com
2. non, je n'ai autorisé jelachemonsmartphone.com qu'à m'afficher le nombre d'heures d'utilisation de mon smartphone, pas à les transmettre à un tiers pour analyse.

Réponse : 2. Le RGPD impose de recueillir le consentement **spécifique**. C'est-à-dire que mon consentement doit correspondre à un seul traitement, pour une finalité déterminée. Je l'ai donné pour afficher le nombre d'heures d'utilisation de mon smartphone? Si jelachemonsmartphone.com veut les vendre ou les donner gentiment à un constructeur, l'application devra alors me demander la permission explicitement pour cet usage précis.

Si je refuse de donner mon consentement à un site pour l'utilisation d'une partie de mes données, celui-ci pourra dégrader en partie son service.

1. oui, un service peut inciter un utilisateur à donner son consentement en lui promettant de lui rétablir une fonctionnalité s'il donne ses données

2. non, ça s'appelle du chantage, on ne négocie pas avec les terroristes

Réponse 2. Le consentement doit être **libre** c'est-à-dire qu'il ne doit pas être contraint ni influencé. La personne doit se voir offrir un choix réel, sans avoir à subir de conséquences négatives en cas de refus. Par exemple, WhatsApp a demandé à ses utilisateur.rice.s l'autorisation de traiter les données pour faire fonctionner son service de messagerie mais a aussi demandé à ses utilisateur.rice.s que celles-ci puissent être traitées par la maison mère Facebook. Si vous refusez ce traitement, Whatsapp ne fonctionne pas. La seule façon de s'opposer au traitement de ses données personnelles par Facebook INC était de désinstaller l'application. C'est tout sauf un consentement libre. Whatsapp s'est d'ailleurs fait remonter les bretelles par la CNIL.

J'ai lu les conditions d'utilisation du service jelachemonsmartphone.com, par contre celles-ci ne sont pas très claires quant au traitement de mes données personnelles.

Je n'arrive pas à comprendre si celles-ci ne vont être affichées que sur mon smartphone pour me rendre compte de mon utilisation quotidienne ou si celles-ci vont être transmises à un tiers. Je lirais bien les conditions d'utilisation en entier mais il y a 152 pages.

1. Dans ces 152 pages il doit y avoir tout le détail d'utilisation de mes données, c'est juste moi qui suis un peu trop bête pour comprendre, mais ça doit être légal
2. 152 pages pour m'expliquer ce qu'ils vont faire avec mes données, c'est beaucoup trop, forcément ils m'enfument

Réponse : 2. Le responsable de traitement des données doit recueillir le consentement **éclairé** des utilisateurs. Le RGPD a introduit une obligation de transparence : un service doit déclarer à ses utilisateur.rice.s :

- l'identité du responsable du traitement de ses données personnelles,
- la finalité du traitement de celles-ci
- l'identité du destinataire des données
- la durée de conservation des données
- L'existence de transferts en dehors de l'UE;
- L'existence des droits d'accès, de rectification, d'effacement, de limitation et d'opposition au traitement et du droit à la portabilité ;
- L'existence du droit d'introduire une réclamation auprès d'une autorité de contrôle (exemple: CNIL)

Pour recueillir mon accord pour traiter mes données, le site

jelachemonsmartphone.com m'a pré-mâché le travail : toutes les cases à cocher des formulaire l'autorisant à traiter mes données sont déjà pré-cochées, je n'ai plus qu'à valider.

1. c'est sympa, ça me fait gagner du temps
2. c'est interdit, certaines personnes vont aller trop vite et juste cliquer sur valider sans avoir compris ce qu'il va être fait de leurs données.

Réponse : 2. Encore une fois, tout acteur de traitement de données doit recueillir le consentement des personnes concernées. Celui-ci doit être libre, spécifique , éclairé et univoque. Univoque signifie que le consentement doit être donné par une déclaration ou tout autre acte positif clair. Ici le choix étant pré-rempli, ce n'est pas ce qu'on appelle un acte positif, donc le consentement n'est pas valide. Plus d'informations sur le consentement sur le site de la CNIL.

Je ne suis plus satisfait de l'application jelachemonsmartphone.com. J'ai trouvé une application bien plus facile à utiliser, jelachemonsmartphoneetjerespecteleRGPD.com. Par contre j'aimerais bien récupérer tout l'historique de l'usage de mon smartphone auprès de jelachemonsmartphone.com pour l'importer dans ma nouvelle application :

1. Je rêve... jelachemonsmartphone.com ne se donnera jamais la peine de me donner mon historique d'utilisation vu que je les lâche
2. Je me débrouille et j'importe tout à la main
3. jelachemonsmartphone.com a l'obligation de me rendre toutes mes données
4. peu importe, mon iPhone X vient de tomber, la vitre est cassée, j'en ai pour un demi SMIC à le faire réparer, j'ai trop le seum,

Réponse : 3. Le RGPD introduit de nouveaux droits pour les utilisateurs.rice. dont le **droit à la portabilité des données**. Ce droit offre aux personnes la possibilité de récupérer une partie de leurs données dans un format ouvert et lisible par machine. Elles peuvent ainsi les stocker ou les transmettre facilement d'un système à un autre en vue de leur réutilisation à des fins personnelles. Ce sont vraiment vos données ! C'est pour cette raison que des services comme Facebook ou Google ont ajouté de nouvelles options de récupération de données pour leurs utilisateurs. Plus d'information sur la portabilité des données sur le site de la CNIL.

J'ai autorisé jelachemonsmartphone.com à partager mes données avec les constructeurs de smartphone pour un usage statistique. J'ai réfléchi et je ne

souhaite plus qu'aucun constructeur ait accès à mes données d'utilisation.

1. Trop tard, les données sont chez les constructeurs, j'ai donné mon accord, je ne peux pas les récupérer
2. Pas grave, j'appelle tous les constructeurs et je leur demande d'effacer mes données. Quelqu'un aurait le 06 du PDG de Huawei ?
3. Je demande à jelachemonsmartphone.com d'effacer les données. Ils ont l'obligation légale de les effacer. Ils contactent le constructeur.

Réponse : 3. Le RGPD prévoit un droit d'effacement. L'utilisateur.rice peut retirer son consentement à tout moment et le responsable du traitement des données a alors l'obligation de les supprimer. Ce n'est pas toujours simple, en témoigne le parcours du combattant pour supprimer son compte Facebook (cf le jeu de l'oie de suppression du parcours Facebook).

Je viens d'apprendre que Jelachemonsmartphone.com s'est fait pirater il y a presque un an et ils ne me préviennent que maintenant !

1. C'est normal, ils ont tellement de travail, ils ne peuvent pas prévenir tout le monde
2. Ce n'est pas si grave, ce ne sont que des données d'utilisation
3. Ils sont hors la loi. Ils auraient dû m'informer de la fuite de mes données
4. peu importe, mon iPhone X vient de tomber, la vitre est cassée, j'en ai pour un demi SMIC à le faire réparer, j'ai trop le seum,

Réponse : 3. Avec le RGPD, les plateformes et les responsables des traitements de données ont l'obligation légale de signaler une violation de données à caractère personnel dans les 72 heures. Le RGPD a été créé pour que les sociétés chez qui nous hébergeons nos données soient responsabilisées et pour qu'elles soient plus loyales envers leurs utilisateur.rice.s. En effet, ces dernières années ont vu se produire de nombreuses fuites de données. Avant le RGPD, les sociétés n'avaient aucune obligation ni de protection des données ni aucune obligation de prévenir leurs utilisateur.rice.s. Par exemple, en 2017, la compagnie Uber s'est fait pirater les données personnelles de 57 millions d'utilisateur.rice.s. Uber n'a prévenu personne, pas même les utilisateur.rice.s et a révélé cette fuite de données 2 ans après. Je vous laisse imaginer les potentiels d'usurpation d'identité ou autres auxquels les client.e.s d'Uber ont pu être confronté.e.s. Y'a t-il des utilisateur.rice.s d'Uber dans la salle ? Peut-être vos données ont-elles également fuité ?

3 En résumé

En France, il existait avant le RGPD une loi sur la protection des données, la loi informatique et libertés de 1978. Cette loi a créé la CNIL, la commission informatique et libertés, un organisme d'État (en fait une autorité administrative indépendante) chargé de protéger nos données personnelles. Le problème est que la CNIL n'avait pas beaucoup de pouvoir de sanction et en cas de non-respect des lois sur les données personnelles, celle-ci ne pouvait mettre des amendes que très limitées. Le RGPD a tout changé. Les organismes de protection des données personnelles ont désormais avec le RGPD la possibilité d'infliger des amendes indexées sur le chiffre d'affaires, ce qui change tout, on l'a vu avec la première amende infligée à Google d'un montant record de 50 millions d'euros.

Avec le RGPD en France, on passe d'une situation déclarative à une situation normative et ça aussi ça change tout. Avant le RGPD les entreprises devaient effectuer une déclaration préalable à la CNIL. Aujourd'hui, les responsables de traitement de données personnelles ont l'obligation de se tenir prêt à tout moment en cas de contrôle à prouver sa conformité avec le RGPD. Pour ceux qui veulent savoir comment s'y préparer, la CNIL a mis en place un guide en 6 étapes.

Côté utilisateur.rice, s'il n'y a qu'une chose à retenir du RGPD, c'est que désormais les services et responsables de traitement de données personnelles ont une obligation de loyauté et d'information envers leurs utilisateur.rice.s. Cette notion se concentre dans le recueil du consentement de l'utilisateur.rice pour le traitement de données qui doit être comme on l'a vu libre, spécifique, éclairé et univoque. Mais maintenant vous savez ce que c'est !