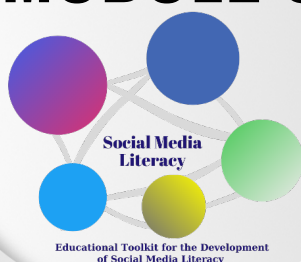


Produit n° 2

Support de cours pour le développement de l'éducation aux médias sociaux dans les écoles

Qu'est-ce que le GDPR?
Qu'est-ce qu'une donnée personnelle ?
Qu'est-ce qu'un traitement ?
Qui doit suivre les règles du GDPR?
Les règles du GDPR
Publicité ciblée/comportementale
Que faire en cas d'infraction ?

MODULE 6



Règles de protection des données dans le contexte des médias sociaux – RGPD

Cofinancé par le
programme Erasmus+
de l'Union européenne



Erasmus+ ref.no. 2019-1-R001-KA201-063996

Le soutien de la Commission européenne à la production de cette publication ne constitue pas une approbation du contenu, qui reflète uniquement le point de vue des auteurs, et la Commission ne peut pas être tenue responsable de toute utilisation qui pourrait être faite des informations qu'elle contient.



Objectif du module

Lorsqu'on se tourne vers les médias sociaux, la protection de la vie privée et des données entre inévitablement en jeu. Le monde numérique d'aujourd'hui nous permet de tout partager avec tout le monde. Tous types de personnes, organisations, entreprises et même le gouvernement traitent des informations vous concernant. Pensez à votre école, votre commune ou votre ville, votre club de sport, votre employeur, etc. La plupart des informations vous concernant sont collectées sur internet. En particulier sur les sites de réseaux sociaux, comme Facebook et Instagram, de nombreuses informations personnelles sont partagées. Une idée fausse très répandue est que les services des plateformes de médias sociaux sont gratuits : en réalité, vous payez, mais au lieu de payer avec de l'argent, vous payez avec vos données personnelles. Si cela peut être un moyen agréable de communiquer avec ses amis et même un moyen amusant de se faire de nouveaux amis, le partage d'informations personnelles comporte également des risques. Tout ce que vous partagez en ligne peut laisser des empreintes numériques. Une fois qu'une photo, une vidéo, un statut, un tweet, etc., est publié sur internet (par exemple sur votre profil de média social), vous n'en avez plus le contrôle : n'importe qui peut copier, rediffuser ou enregistrer la photo, ce qui rend impossible de l'effacer complètement d'internet. Ces empreintes numériques peuvent être des "données personnelles" (par exemple, votre nom, votre adresse (électronique), votre date de naissance, vos photos). Le partage de ce type de données peut vous exposer à toutes sortes de risques (par exemple, l'usurpation d'identité, le harcèlement, l'hyper exposition au contenu personnalisé, la publicité ciblée et bien plus encore). Il est donc important de savoir quelles données personnelles vous concernant sont collectées, de quelle manière, pendant combien de temps et ce qui est fait pour protéger vos données personnelles. C'est là que le législateur est intervenu.

Vos données personnelles ne peuvent pas simplement être utilisées par d'autres, et vous ne pouvez pas non plus utiliser les données personnelles d'autres personnes. Depuis un certain temps déjà, des lois sur la protection de la vie privée limitent l'utilisation des données personnelles. En raison de l'essor des médias sociaux, d'autres plateformes en ligne, des applications mobiles, etc. - qui reposent toutes sur le traitement de grandes quantités de données à caractère personnel, ces lois sont devenues obsolètes et n'étaient plus en mesure d'assurer une protection suffisante des personnes et de leurs données personnelles. Ces lois nationales ont donc été remplacées par le règlement général sur la protection des données (RGPD), qui s'applique dans toute l'Union européenne.





Le RGPD oblige toute personne qui traite des données personnelles à se conformer aux règles du règlement, ce qui inclut également les écoles et les enseignants. Les enfants passant une grande partie de leur temps sur les médias sociaux et les écoles étant d'importants collecteurs de données personnelles (sur leur personnel et leurs élèves et en ligne comme hors ligne), ce module revêt une grande importance. Vie privée et protection des données sont des droits fondamentaux pour tous. Il est important que les jeunes connaissent le RGPD et soient conscients de leurs droits et obligations à cet égard. Les enseignants étant souvent un premier point de contact pour les élèves, ils sont dans une position clé pour informer et sensibiliser les élèves au RGPD.

Nombre d'heures : 2

Résultats d'apprentissage

- Sensibiliser et familiariser les élèves et les enseignants avec le RGPD, son objectif et son importance ;
- Connaissance des obligations des entreprises et des organisations en matière de traitement des données personnelles en vertu du RGPD ;
- La connaissance de leurs propres droits en ce qui concerne le traitement de leurs données personnelles ;
- Compréhension du concept et de la valeur des "données personnelles" et du "traitement" ;
- Créer un réflexe naturel chez les élèves pour qu'ils réfléchissent, avant de partager des données personnelles, à la question de savoir si les informations qu'ils ont l'intention de partager ne sont pas trop personnelles et ne constituent pas un risque pour leur vie privée ;
- Ce que l'on peut/doit trouver dans une politique de confidentialité ;
- L'aptitude d'utiliser les paramètres de confidentialité de leur plateforme de médias sociaux afin de s'assurer que seules les personnes de leur choix peuvent voir les informations de leur profil ;
- Comprendre la publicité ciblée ;
- Développer la connaissances des écoles et des enseignants sur la manière d'utiliser légalement les médiassociaux ;
- Développer la connaissance de ce qu'il faut faire en cas d'utilisation illégale de données personnelles ;





Matériel de formation

Contexte

1.1. Qu'est-ce que le RGPD ?

Le règlement général sur la protection des données est entré en vigueur le 25th mai 2018 et s'applique à toute organisation établie dans l'UE ou établie en dehors de l'UE mais qui traite des données personnelles de personnes de l'UE - cela inclut les écoles ou tout autre établissement d'enseignement. Grâce à l'introduction de nouvelles règles, le RGPD vise à redonner aux individus le contrôle de leurs données personnelles en limitant la façon dont d'autres personnes et organisations peuvent utiliser vos données personnelles.

Le RGPD protège vos données personnelles à partir du moment où vous partagez ces données avec d'autres personnes. Les autres ne sont pas simplement autorisés à partager, enregistrer, copier, lier... ces données. Le RGPD définit des règles que les entreprises, les organisations et les gouvernements doivent suivre dans le cas où ils souhaiteraient utiliser les données personnelles des individus : le traitement doit être effectué de manière légale, équitable et transparente. En outre, le RGPD établit un certain nombre de droits pour aider les individus à garder le contrôle de leurs données personnelles.

Étant donné que le partage d'informations personnelles sur les sites de réseaux sociaux ou l'échange de données personnelles pour l'accès à des applications et à d'autres services en ligne sont aujourd'hui monnaie courante, ce module se concentrera sur le RGPD et la protection des données à la lumière de ces services.

1.2. Qu'est-ce qu'une donnée personnelle ?

1.2.1. En général





Les données personnelles sont toutes sortes d'informations qui révèlent quelque chose sur vous personnellement. Par exemple, le nom, le numéro d'identification, la date de naissance, l'adresse, les données de localisation, les photos ou vidéos d'une personne, la religion, l'adresse IP, l'historique de navigation, les marques, les fiches de comportement, les profils de médias sociaux (y compris vos goûts, vos partages et vos amis) etc.

Cette notion doit être interprétée de manière très large : s'il est possible d'identifier un individu directement ou indirectement à partir des informations concernées, alors ces informations sont des données à caractère personnel.

- Identification directe :

Les informations permettent en elles-mêmes d'identifier la personne à laquelle ces informations se rapportent.

Par exemple, nom, numéro de téléphone, numéro d'identification, adresse du domicile, adresse électronique, données de localisation, enregistrements vocaux, etc.

- Identification indirecte :

L'information, en tant que telle, ne suffit pas à identifier une personne, mais la prise en compte d'informations supplémentaires - déjà disponibles ou devant être obtenues auprès d'une autre source - permet d'identifier la personne concernée.

Par exemple, les plaques d'immatriculation peuvent être considérées comme des données à caractère personnel, indépendamment du fait que vous n'avez pas vous-même accès aux bases de données reliant les plaques d'immatriculation aux propriétaires des voitures. Le fait que d'autres personnes puissent établir ce lien suffit à qualifier ces informations de données à caractère personnel. Le même raisonnement s'applique aux informations collectées par les cookies, les identifiants numériques et les adresses MAC et IP (qui sont uniques à un appareil).

Une seule information (par exemple, la couleur des cheveux, la profession, la voiture...) peut ne pas permettre d'identifier une personne physique en tant que telle, mais il peut en être autrement lorsque cette donnée est combinée à d'autres. Les entreprises qui collectent plusieurs types de données sur les personnes (par exemple, les médias sociaux) doivent en tenir compte.





Données personnelles
Informations relatives à une <u>personne physique</u> Pas d'informations sur les entreprises et autres organisations, les personnes décédées, les animaux domestiques, les objets, etc.
<u>Le format n'a aucune importance</u> : texte, image, vidéo, son, etc.
Les informations permettent d'identifier une seule personne, soit <u>directement</u> , soit <u>indirectement</u> (par la prise en compte d'informations complémentaires)

1.1.1. Catégories particulières de données à caractère personnel

Le RGPD fait la distinction entre les données personnelles "ordinaires" et les catégories spéciales de données. En raison de la nature sensible de ces dernières et de leur fort potentiel d'impact négatif sur la vie privée d'une personne et sur d'autres libertés et droits fondamentaux (par exemple, le droit de ne pas être discriminé) lorsqu'elles sont utilisées, le traitement de ce type de données personnelles est, en principe, interdit.





1.1.1. Pourquoi les données personnelles sont-elles précieuses ?

Les données personnelles sont souvent appelées "le pétrole de d'internet" et la nouvelle monnaie du monde numérique d'aujourd'hui. En d'autres termes, les données personnelles sont considérées comme extrêmement précieuses. De nombreuses entreprises proposent leurs services en ligne gratuitement, tandis qu'elles gagnent leur vie grâce à la publicité. C'est la publicité qui profite principalement du traitement des données personnelles.

Lorsque vous allez sur internet, vous laissez des empreintes numériques. L'état de la technologie actuelle permet aux entreprises d'utiliser et de stocker les données personnelles que vous générez lorsque vous achetez certains biens ou services, ou simplement en recherchant certaines choses ou informations (votre nom, vos centres d'intérêt, vos souhaits, votre style, etc.) Un certain nombre de clics et de "likes" sur les médias sociaux (par exemple Facebook) suffisent aux entreprises pour effectuer une analyse visant à déterminer vos préférences exactes. En combinant toutes ces informations provenant de différentes sources, les entreprises sont en mesure de dresser un portrait clair de vous. C'est là que l'on voit la valeur des données personnelles : si une entreprise sait ce que vous recherchez ou ce qui vous intéresse, elle est en mesure d'obtenir des informations plus précises. être en mesure de vous envoyer spécifiquement des publicités pour ces produits ou services. *(Plus d'informations à ce sujet sous 4. Publicité ciblée)*

Les données personnelles n'intéressent pas seulement les entreprises, mais aussi les pirates informatiques ! Ces dernières années, plusieurs grandes entreprises ont fait l'actualité à la lumière de scandales de piratage, à l'occasion desquels des données personnelles de leurs clients ont été volées (par exemple Cambridge Analytica, Facebook , Mastercard).

Enfin, les données personnelles fournissent également des informations intéressantes pour les autorités publiques, car elles peuvent leur permettre d'obtenir de nouvelles informations sur des individus ou des groupes d'individus.

Une utilisation incontrôlée des données personnelles pourrait toutefois placer les entreprises privées, les pirates informatiques et les autorités publiques en position de force.

12. Qu'est-ce que le traitement ?

Les règles du RGPD ne s'appliquent qu'au traitement des données personnelles.

Traitement = toute opération ou ensemble d'opérations effectuées sur des données à caractère





personnel ou sur des ensembles de données à caractère personnel, que ce soit ou non par des moyens automatisés.

Par exemple, la collecte, l'enregistrement, l'organisation (par exemple, la création d'une liste de diffusion), la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition (par exemple, la publication d'un message ou d'une photo sur la page Facebook d'une organisation), l'alignement ou la combinaison, la restriction, l'effacement ou la destruction de données à caractère personnel.

Si l'une des actions susmentionnées est réalisée sur vos données personnelles, le RGPD s'applique.

Il est important de noter que le traitement pour des activités purement personnelles ou domestiques ne relève pas du RGPD. (par exemple, des parents prenant des photos de leur enfant et de ses camarades de classe lors d'un événement scolaire pour les conserver à la maison dans un album photo).

1.3. Qui doit suivre les règles du RGPD ?

Le RGPD s'applique à une entreprise ou une entité (c'est-à-dire une personne physique ou morale, une autorité publique, une agence ou un autre organisme), quels que soient leur taille, leur secteur, leur nombre d'employés ou leur chiffre d'affaires, qui :

- traite des données à caractère personnel dans le cadre des activités de l'une de ses succursales établies dans l'UE (quel que soit le lieu où les données sont traitées) ;
- est établi en dehors de l'UE et traite des données à caractère personnel dans le but d'offrir des biens/services à des personnes de l'UE ou de surveiller le comportement de personnes de l'UE.

Ces entreprises ou entités sont considérées comme les responsables du traitement de vos données personnelles et doivent veiller à ce que le RGPD soit respecté.





Les règles

2.1. Les principes du RGPD

Toute entreprise ou entité traitant des données personnelles devra suivre certaines règles.

2.1.1. Légalité, équité et transparence

(a) Légalité

Lorsqu'une entreprise ou une organisation souhaite traiter vos données personnelles, elle doit, avant de le faire, s'assurer que son traitement peut être fondé sur un motif de justification - une **base licite** - en vertu du RGPD. Une base licite est une raison pour le traitement qui est déterminée et acceptée par le RGPD (voir l'article 6 du RGPD).

Les plus pertinentes de ces bases légales à la lumière des médias sociaux sont les suivantes : le traitement des données personnelles est nécessaire **à l'exécution d'un contrat**, la société ou l'organisation a obtenu votre **consentement**, ou la société ou l'organisation a un **ou plusieurs intérêts légitimes** à traiter vos données personnelles.

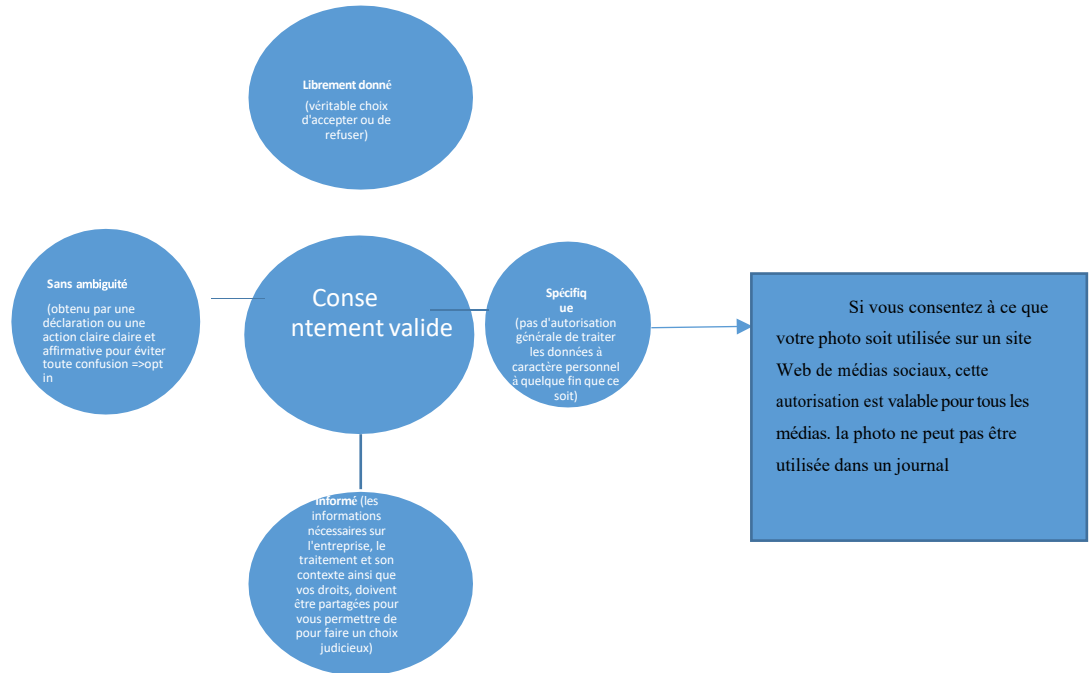
Nécessité contractuelle

Lorsqu'une entreprise ou une organisation doit traiter des données à caractère personnel pour se conformer à des obligations contractuelles entre elle et vous, ou pour exécuter des demandes précontractuelles de votre part, elle peut se fonder sur la base légale "contrat". Certaines obligations contractuelles ne peuvent tout simplement pas être exécutées sans collecter et traiter certaines données à caractère personnel. Les traitements utiles, mais non objectivement nécessaires, à l'exécution du service contractuel ou à l'accomplissement de démarches précontractuelles pertinentes ne sont pas couverts par cette base légale.

Exemple : Twitter traite vos données personnelles - telles que votre nom et votre adresse électronique - afin de créer votre compte, à des fins d'authentification et pour permettre la création de contenu

Consentement

Le consentement a une signification particulière dans le cadre du RGPD. Pour être valable, le consentement doit être :



Vous devez pouvoir retirer votre consentement à tout moment. Les informations sur la manière de le faire doivent être fournies au moment où il vous est demandé de consentir à une certaine activité de traitement. La manière de retirer son consentement doit être aussi simple que de donner son consentement et ne doit pas entraîner de conséquences négatives pour vous (par exemple, des frais ou des niveaux de service inférieurs).

Exemple : Facebook dispose d'une fonctionnalité de reconnaissance faciale qui permet au réseau social de vous reconnaître sur les photos ou vidéos présentes sur sa plateforme. L'utilisation d'une telle fonctionnalité entraîne le traitement de données à caractère personnel, à savoir des photos ou des vidéos de vous. Pour activer cette fonction, Facebook vous demande votre consentement.



Il en va de même pour la fonction "historique de localisation" proposée par Facebook. Lorsque vous consentez à l'utilisation de cette fonction, vos données de localisation sont traitées afin d'explorer ce qui se passe autour de vous, de vous montrer des publicités pertinentes, de rechercher des amis dans les environs.

Exemple : Twitter traite les informations qu'il recueille auprès de vous sur Twitter, votre autre activité en ligne, et les données de leurs partenaires afin de diffuser des publicités personnalisées sur et hors Twitter, sur la base de votre consentement.

Une entreprise ou une organisation ne peut traiter les données personnelles d'un enfant que sur la base du consentement avec le consentement explicite de leur parent ou tuteur jusqu'à un certain âge. Le seuil d'âge pour obtenir le consentement des enfants peut varier de 13 à 16 ans selon les pays de l'UE. (Vous pouvez vérifier ce point auprès de votre autorité nationale chargée de la protection des données).

Intérêt légitime

Les intérêts légitimes pour lesquels il est **nécessaire de** traiter les données à caractère personnel peuvent être vos propres intérêts ou les intérêts de tiers (par exemple, des intérêts commerciaux, des intérêts individuels ou des avantages sociétaux plus larges). Cet intérêt doit être spécifié dans la politique de confidentialité.

Pour invoquer valablement ce motif de traitement, les entreprises ou organisations doivent traiter vos données d'une manière à laquelle vous vous attendriez raisonnablement, sans vous causer de préjudice injustifié. Si ce n'est pas le cas, il est probable que vos intérêts l'emportent sur ceux de la société ou de l'organisation, ce qui signifie qu'elles ne sont pas autorisées à traiter vos données personnelles (sur cette base légale), à moins qu'il n'existe une justification impérieuse pour le traitement.

Exemple : Twitter fait des déductions sur votre compte – telles que les centres d'intérêt, l'âge et le sexe – afin de fournir des fonctionnalités telles que les suggestions de compte, la publicité, la recommandation, la chronologie, le classement etc...





Exemple : YouTube (Google) traite vos données personnelles pour ses intérêts légitimes et ceux de tiers, tout en appliquant les garanties appropriées qui protègent votre vie privée. C'est par exemple le cas pour personnaliser leurs services afin de vous fournir une meilleure expérience utilisateur marketing pour informer les utilisateurs sur leurs services, mais aussi pour fournir de la publicité, ce qui maintient la gratuité de bon nombre de leurs services. (Lorsque les publicités sont personnalisées, elles demandent le consentement.)

Catégories particulières de données

Il est important d'ajouter que pour les catégories spéciales de données personnelles, il existe 10 exceptions à l'interdiction générale de traiter ces données (voir l'article 9 du RGPD). Si l'une de ces conditions est remplie, les catégories spéciales de données peuvent être traitées légalement. L'exception la plus importante à la lumière des médias sociaux est lorsqu'il y a un **consentement explicite** de la personne dont les données personnelles sont concernées.

Ces exceptions forment une couche supplémentaire de conditions en plus des règles habituelles. En pratique, cela signifie que lorsque vous souhaitez traiter des catégories particulières de données, il doit y avoir une base légale (art. 6) et une exception doit être applicable (art. 9).

Exemple : YouTube (Google) traite vos données personnelles pour ses intérêts légitimes et ceux de tiers, tout en appliquant les garanties appropriées qui protègent votre vie privée. C'est par exemple le cas pour personnaliser leurs services afin de vous fournir une meilleure expérience utilisateur marketing pour informer les utilisateurs sur leurs services, mais aussi pour fournir de la publicité, ce qui maintient la gratuité de bon nombre de leurs services. (Lorsque les publicités sont personnalisées, elles demandent le consentement.)

(b) Équité

La société ou l'entité qui traite vos données personnelles doit le faire de manière équitable, ce qui signifie d'une manière à laquelle vous pourriez raisonnablement vous attendre et non d'une manière qui cause des effets négatifs injustifiables ou vous induit en erreur. (c)

(c) Transparence

Il s'agit d'un principe très important, qui est lié à la loyauté ! Dès le départ, les entreprises ou organisations doivent être claires, ouvertes et honnêtes avec vous sur la manière dont elles utiliseront vos données personnelles. Pour cela, les informations doivent être fournies dans un





langage facilement accessible et compréhensible. C'est là que la politique de confidentialité entre en jeu. Les politiques de confidentialité longues et compliquées sont à éviter selon le RGPD.

Une politique de confidentialité

La politique de confidentialité est l'endroit à consulter lorsque vous souhaitez obtenir des informations sur la manière dont vos données personnelles sont collectées, utilisées et protégées par les médias sociaux (ou tout autre site web). Toute politique de confidentialité doit contenir un grand nombre de mentions obligatoires :

- nom et coordonnées de l'entreprise/organisation
- les coordonnées du délégué à la protection des données, s'il en existe un
- leur(s) objectif(s) de traitement des données personnelles et la base légale sur laquelle ils se fondent pour traiter les données
- l'intérêt légitime du traitement (le cas échéant)
- les (catégories de) données personnelles obtenues (si elles ne sont pas obtenues directement auprès de vous)
- les (catégories de) destinataires des données personnelles (les données personnelles seront-elles partagées avec d'autres parties ?)
- les détails des transferts de données à caractère personnel vers tout pays tiers ou organisation internationale (le cas échéant)
- la durée de conservation des données (période de conservation)
- les droits que vous pouvez exercer (par exemple, droit d'accès, droit d'oubli, droit de rectification, etc.)
- le droit de retirer le consentement (le cas échéant)
- votre droit de déposer des plaintes auprès de l'autorité de protection des données
- La source des données personnelles (si les données personnelles ne sont pas obtenues directement auprès de vous)
- Les détails de l'existence d'une prise de décision automatisée, y compris le profilage (le cas échéant).





2.1.2. Limitation de la finalité du traitement

Le principe de limitation de la finalité signifie que les entreprises ou les organisations doivent clairement définir une finalité spécifique pour chacune de leurs activités de traitement, avant de commencer. Cette exigence vise à assurer la transparence, la prévisibilité et le contrôle des utilisateurs. Tout traitement de données à caractère personnel doit être effectué pour une finalité spécifique bien définie ou pour des finalités supplémentaires, spécifiées et compatibles avec la finalité initiale. Le traitement de données à caractère personnel à des fins non définies et/ou illimitées est donc illégal.



Chaque nouvelle finalité du traitement des données à caractère personnel qui n'est pas compatible avec la finalité initiale doit avoir sa propre base légale particulière et ne peut pas se fonder sur le fait que les données ont été initialement acquises ou traitées pour une autre finalité légitime.

Exemple : Si vous autorisez Facebook à utiliser la fonction de reconnaissance faciale afin de repérer des photos et des vidéos sur la plate-forme avec vous, cela ne signifie pas que Facebook peut utiliser ces données dans le but de vous fournir des publicités ciblées basées sur cela. données personnelles. Il aura besoin d'une base légale distincte (par exemple, le consentement) pour cela.

2.1.3. La minimisation des données

Les entreprises et les organisations ne peuvent traiter que les données personnelles dont elles ont réellement besoin pour atteindre leur objectif spécifié, pas plus. Cela signifie qu'elles devront régulièrement revoir les données qu'elles stockent afin de supprimer tout ce dont elles n'ont pas besoin.

2.1.4. Précision

Les entreprises et les organisations doivent prendre des mesures raisonnables pour s'assurer que les données personnelles qu'elles détiennent sont correctes et non trompeuses. Cela implique qu'elles devront tenir les données personnelles à jour, en les corrigeant ou en les supprimant, le cas échéant.

2.1.5. Limitation du stockage

Les données personnelles ne peuvent pas être conservées éternellement. Les entreprises et les organisations doivent supprimer ou rendre anonymes les données personnelles dès qu'elles n'en ont plus besoin pour atteindre le ou les objectifs pour lesquels les données ont été collectées. Les entreprises et les organisations doivent réfléchir dès le départ à la durée de conservation de vos données personnelles et à la justification de cette durée, qui dépendra de la finalité du traitement. Des informations à ce sujet devraient figurer dans les politiques de confidentialité.

2.1.6. Intégrité et confidentialité (sécurité des données)

La protection des données à caractère personnel contre tout traitement non autorisé ou illicite, toute perte accidentelle, toute destruction ou tout dommage est au cœur de ce principe d'intégrité et



de confidentialité (sécurité des données). Le principe de sécurité des données vise à éviter les effets négatifs pour vous en obligeant la mise en œuvre de mesures techniques (par exemple, le cryptage, la pseudonymisation) et/ou organisationnelles (par exemple, en veillant à ce que les données personnelles ne soient pas accessibles à tout le monde au sein d'une organisation, mais uniquement à ceux qui doivent travailler avec ces données).

2.1.4. Responsabilité

Le principe de responsabilité exige que les entreprises ou les organisations assument la responsabilité de ce qu'elles font avec vos données personnelles et de la manière dont elles se conforment au RGPD. À la lumière de ce principe, elles doivent mettre en place des mesures et des enregistrements qui leur permettent de démontrer leur conformité lorsqu'on leur demande de le faire.





Vos droits

Dans la société numérisée d'aujourd'hui, il est important de connaître ses droits en matière de protection des données.

3.1. Le droit d'être informé

Les entreprises et les organisations doivent vous informer sur la collecte et l'utilisation de vos données personnelles. Ceci est lié au principe de transparence qui sous-tend le RGPD. Voir 2.1.1.(c) sur les informations à fournir.

L'information doit être communiquée :

- au moment où vous recueillez leurs données personnelles.
- au plus tard un mois après avoir obtenu les données, dans le cas où vous recevez les données personnelles depuis quelqu'un d'autre.

Les informations doivent être concises, transparentes, intelligibles, facilement accessibles et doivent utiliser un langage clair et simple. Ces informations sont principalement fournies via une politique de confidentialité.

3.2. Le droit d'accès

Vous avez le droit d'accéder aux données personnelles vous concernant, détenues par une entreprise ou une organisation. En pratique, cela signifie que vous recevrez les informations suivantes :

- Si l'entreprise ou l'organisation traite ou non vos données personnelles
- Une copie de ces données (généralement, gratuitement)





- Informations supplémentaires : les entreprises ou organisations doivent vous fournir les mêmes informations que celles qui doivent figurer dans une politique de confidentialité (voir 2.1.1.(c)).

L'exercice de ce droit vous aide à comprendre comment et pourquoi les entreprises ou organisations utilisent vos données, et à vérifier si elles le font en conformité avec le RGPD.

Il est possible pour l'entreprise ou l'organisation de refuser l'accès lorsque la demande est manifestement infondée (par exemple, elle n'est manifestement faite que pour harceler l'entreprise) ou excessive (par exemple, elle chevauche d'autres demandes). Les raisons du refus doivent vous être clairement communiquées. Les entreprises et les organisations ont un mois pour répondre à la demande.

3.3. Le droit à l'effacement ("droit à l'oubli")

Le RGPD vous accorde le droit de faire effacer vos propres données personnelles. Ce droit est lié aux principes de minimisation et d'exactitude des données, obligeant les entreprises et les organisations à envisager d'effacer les données personnelles à certaines occasions. Vous pouvez exercer votre droit à l'effacement lorsque :

- vos données personnelles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées par la société ou l'organisation ;
- Lorsque l'entreprise ou l'organisation s'appuie sur votre consentement comme base légale pour détenir les données, et que vous souhaitez retirer votre consentement ;
- Lorsque l'entreprise ou l'organisation se fonde sur des intérêts légitimes comme base légale du traitement, vous pouvez vous opposer au traitement de vos données, et s'il n'y a pas d'intérêt légitime prépondérant à poursuivre ce traitement, vos données seront effacées ;
- Lorsque l'entreprise ou l'organisation traite les données personnelles pour vous envoyer du marketing direct et que vous vous opposez à ce traitement ;
- Lorsque vos données personnelles ont été traitées de manière illégale (= sans s'appuyer correctement sur une base légale valide) ;
- Lorsqu'il existe une obligation légale obligeant l'effacement de vos données personnelles ;
- Lorsque vos données personnelles ont été collectées auprès de vous lorsque vous étiez enfant afin d'offrir des services en ligne.





L'accent est mis en particulier sur le droit à l'effacement si la demande concerne des données collectées auprès d'enfants. Si le consentement au traitement des données à caractère personnel a été donné à l'origine lorsque vous étiez enfant (sans être pleinement conscient des risques), il peut être très important de pouvoir retirer son consentement et faire supprimer les données personnelles. *(Chaque élève peut probablement penser à quelque chose qu'il a publié en ligne dans le passé et avec lequel il n'est plus d'accord ou qu'il trouve embarrassant aujourd'hui).*

L'entreprise ou l'organisation n'est pas obligée de toujours (entièrement) accéder à votre demande car, dans certains cas, le droit à l'effacement ne s'applique pas (par exemple, si le traitement est nécessaire pour se conformer à la loi ou lorsque le traitement a lieu à des fins d'archivage dans l'intérêt public ou pour des recherches scientifiques ou historiques dans le cas où l'effacement entraînerait une atteinte grave à la recherche). Une entreprise ou un organisme peut également refuser l'exercice de votre droit à l'effacement lorsque la demande est manifestement infondée ou excessive (voir 3.2).

Il convient de souligner que, même avec ce droit à l'oubli, il sera très difficile (voire impossible) de supprimer complètement vos données personnelles sur internet. En effet, les données sont souvent partagées (de manière non légale) par des entreprises et des organisations avec d'autres parties qui les partagent à leur tour avec d'autres parties, et ainsi de suite.

3.4. Le droit de rectification

Sur la base du droit de rectification, vous pouvez corriger toute erreur dans vos données personnelles détenues par des entreprises ou des organisations : les données personnelles inexactes peuvent être rectifiées et les données incomplètes peuvent être complétées. Ce droit est clairement lié au principe d'exactitude que les entreprises et les organisations doivent prendre en compte.

Là encore, les entreprises et les organisations ne sont pas toujours tenues d'accéder à votre demande. S'ils estiment que vos données personnelles sont exactes, ils doivent vous le dire et expliquer leur décision. Une autre raison de ne pas accéder (entièrement) à votre demande de rectification peut être le fait que votre demande est manifestement infondée ou excessive (voir 3.2).

3.5. Le droit à la limitation du traitement

Ce droit est une alternative à la demande d'effacement des données à caractère personnel. Il vous permet d'exiger de l'entreprise ou de l'organisation qu'elle cesse de traiter (certaines) de vos





données à caractère personnel, généralement pour une période donnée, le temps de résoudre d'autres problèmes. Ce droit implique que l'entreprise ou l'organisation ne peut que conserver vos données personnelles, sans les utiliser davantage. Les entreprises et organisations ont également la possibilité de refuser la demande de limitation du traitement, avec l'obligation de fournir une explication à ce sujet. L'un des motifs de refus peut à nouveau être le fait que la demande est manifestement infondée ou excessive (voir 3.2).

3.6. Le droit à la portabilité des données

Ce droit vous donne la possibilité d'obtenir et de déplacer vos données personnelles - que vous avez fournies à l'entreprise ou à l'organisation - ailleurs. En pratique, cela signifie que vous pouvez facilement déplacer, copier ou transférer vos propres données personnelles d'un environnement informatique à un autre, de manière sûre et sécurisée et d'une manière couramment utilisée, ou que vous pouvez demander à l'entreprise ou à l'organisation de le faire.

Ce droit ne s'applique que lorsque l'entreprise ou l'organisation se fonde sur le "consentement" ou la "nécessité contractuelle" comme base légale pour traiter ces données à caractère personnel, ou lorsqu'elles sont traitées par des moyens automatisés (c'est-à-dire au moyen de programmes et d'outils informatiques spécialisés et non sur papier, par exemple).

Les entreprises et organisations ont également la possibilité de refuser la demande de limitation du traitement, avec l'obligation de fournir une explication à ce sujet. L'un des motifs de refus peut à nouveau être le fait que la demande est manifestement infondée ou excessive (voir 3.2).

3.7. Droit d'opposition

Le droit d'opposition n'est pas un droit général. Vous pouvez invoquer votre droit d'opposition au traitement de vos données personnelles en fonction de votre situation particulière et aux données traitées dans le but de vous fournir du marketing direct. Cela vous permet d'arrêter ou d'empêcher les entreprises et les organisations de traiter (une partie de) vos données personnelles.

Le droit de s'opposer au traitement à des fins de marketing direct est un droit absolu, ce qui signifie que les entreprises et les organisations doivent toujours accéder à cette demande. Lorsque le droit d'opposition est exercé pour une autre raison, les entreprises et organisations peuvent décider





de continuer à traiter vos données personnelles si elles peuvent prouver qu'il existe une raison impérieuse de le faire. Les entreprises et les organisations ont également la possibilité de refuser la demande de limitation du traitement, sous réserve de l'obligation de fournir une explication à ce sujet. L'un des motifs de refus peut encore être le fait que la demande est manifestement infondée ou excessive (voir 3.2).

3.8. Les droits liés à la prise de décision automatisée, y compris le profilage

Le profilage consiste à évaluer vos aspects personnels afin de faire des prédictions sur vous.

Exemple : Un site Web de médias sociaux évalue certaines informations vous concernant (telles que votre âge, votre sexe, votre taille) et, en fonction de cela, vous classe dans un certain groupe pour la recommandation de contenu ou la publicité.

La prise de décision basée uniquement sur des moyens automatisés fait référence à la situation où la technologie elle-même prend des décisions à votre sujet par la technologie, sans aucune implication humaine. Ceci peut être fait sans profilage.

Sur la base du RGPD, vous avez le droit de ne pas faire l'objet d'une décision basée uniquement sur des moyens automatisés, si la décision entraîne des effets juridiques (c'est-à-dire que vos droits légaux sont impactés) vous concernant ou vous affecte de manière significative de façon similaire (c'est-à-dire qu'elle influence votre situation, votre comportement ou vos choix). Étant donné que ces décisions sont susceptibles d'avoir un impact significatif sur votre vie (elles peuvent concerner, par exemple, la solvabilité, le recrutement en ligne, les performances au travail), une protection spéciale est nécessaire.

Exemple : Les compagnies d'assurance analysent les publications sur les réseaux sociaux de clients (potentiels) à l'aide d'un algorithme recherchant certains mots et expressions indiquant un comportement prudent ou en bonne santé pour vous attribuer un niveau de risque afin de décider de la prime d'assurance.





3.9. En pratique

Lorsque vous exercez vos droits, les entreprises et les organisations disposent d'un mois pour répondre à vos demandes et fournir des informations à l'appui de leur décision. Les demandes doivent être déposées auprès de l'entreprise ou de l'organisation, verbalement ou par écrit (généralement par le biais d'un courriel ou d'une section spécifique du site web. site web). Il devrait être aussi facile d'exercer ces droits que de fournir vos données personnelles en premier lieu.

Publicité ciblée/comportementale

Dans le passé, les entreprises investissaient principalement dans la publicité à la télévision et à la radio. L'inconvénient est que tout le monde reçoit la même publicité, qu'elle soit intéressante ou non, ce qui n'est pas très efficace. Aujourd'hui, les médias sociaux et les progrès technologiques permettent aux entreprises de choisir de faire de la publicité ciblée pour leurs produits et services auprès des consommateurs : par exemple, une publicité pour des chaussures de course n'est présentée qu'aux utilisateurs de médias sociaux qui vont régulièrement courir, et les jours où il ne pleut pas. Ces publicités ciblées peuvent être trouvées sur votre fil d'actualité de médias sociaux ou sur le côté de celui-ci, et peuvent être reconnues par des mots tels que "sponsorisé".

Lesquelles de vos données sont utilisées pour la publicité ?

1. Les données personnelles que vous saisissez lors de la création de votre compte de média social (par exemple, votre âge, votre lieu de résidence, votre date de naissance).
2. Tout ce que vous publiez sur votre compte de médias sociaux, comme des photos, des vidéos et des commentaires. Par exemple, si vous publiez quelque chose comme "J'ai tellement faim en ce moment", il est possible que vous receviez une publicité d'une chaîne de restauration rapide ;
3. Les choses que vous faites et recherchez en dehors de la plateforme de médias sociaux. Par exemple, si vous visitez le site web d'un certain événement, vous pouvez recevoir des publicités concernant cet événement ou un événement similaire sur votre compte de médias sociaux. Cette dernière possibilité est rendue possible par les "cookies".





Les cookies sont de petits fichiers stockés sur votre ordinateur, portable, smartphone ou tablette afin de garder une trace des sites web que vous visitez. Notez que les entreprises doivent demander votre autorisation avant d'utiliser des cookies publicitaires (il existe également d'autres types de cookies). Si vous ne souhaitez pas être suivi sur différents sites web en ligne, vous devez penser à refuser les cookies. L'utilisation de cookies et d'autres technologies de suivi est réglementée par les règles de la vie privée en ligne, et non par le GDPR.

Il est important d'ajouter ici que certaines entreprises de médias sociaux possèdent plusieurs plateformes et, par conséquent, elles peuvent utiliser les informations obtenues à votre sujet sur les deux plateformes (Facebook et Instagram par exemple) ;

4. Votre localisation (en temps réel). Les plateformes de médias sociaux peuvent même voir où vous êtes, en se basant sur le wifi et le gps-tracker de votre téléphone. Vous pourriez ainsi recevoir des publicités pour une certaine salle de sport, si vous vous trouviez à proximité de celle-ci.

Toutes les informations mentionnées ci-dessus sont mémorisées et interprétées par des algorithmes, et bien sûr pas par des êtres humains réels. Sur la base de ces données, les entreprises qui choisissent de faire de la publicité sur les médias sociaux peuvent choisir un "groupe cible" (par exemple, les garçons de 16 ans de la région d'Amsterdam qui aiment le football). La bonne publicité, au bon moment et au bon endroit, peut sérieusement influencer votre comportement, ce qui profite aux entreprises. Bien que la publicité personnalisée ne doive pas toujours être perçue comme une mauvaise chose, il convient de s'en méfier. En particulier lorsque des données sensibles sont en jeu (par exemple, la race, les préférences politiques, etc.), ce type de publicité peut s'avérer délicat et vos données personnelles peuvent même être utilisées à mauvais escient (par exemple, en vous ciblant avec un contenu faux, afin de modifier ou de radicaliser vos préférences politiques).

Que faire en cas d'infraction ?

Quelqu'un a-t-il illégalement partagé vos données personnelles ? a créé un faux profil de vous sur les médias sociaux ? Ou, peut-être avez-vous essayé d'exercer l'un de vos droits au titre du RGPD, mais n'êtes pas satisfait de la réponse de l'entreprise ou de l'organisation ? Tout d'abord, vous pouvez toujours demander à la personne qui enfreint vos droits en matière de protection des





données, de supprimer ou de corriger les données personnelles concernées (par exemple, une photo, un faux profil, des coordonnées). Si rien ne se passe, vous pouvez vous adresser à la plateforme de médias sociaux pour qu'elle supprime ou corrige les données à caractère personnel. Si ces démarches ne sont pas satisfaisantes, vous pouvez déposer une plainte auprès de votre autorité nationale de protection des données. (Une autre option consiste à faire valoir vos droits par un recours judiciaire).

Chaque pays de l'UE possède sa propre autorité de protection des données. Vous pouvez en trouver la liste ici : https://edpb.europa.eu/about-edpb/board/members_en

Les autorités chargées de la protection des données sont des autorités publiques indépendantes qui contrôlent et supervisent si les entreprises et les organisations sur leur territoire appliquent correctement les règles de protection des données. Elles fournissent également des conseils d'experts sur les questions de protection des données et traitent les plaintes des personnes.

comme vous. Les autorités peuvent prononcer des avertissements, des réprimandes, une interdiction temporaire ou définitive de traitement et des amendes (très élevées).

Sur les sites web de ces autorités chargées de la protection des données, vous trouverez la marche à suivre pour déposer une plainte, par téléphone, par courrier électronique ou au moyen d'un formulaire de contact disponible sur leur site web.

Ressources

- https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_fr.pdf (Manuel général sur la protection des données)
- <https://www.youtube.com/watch?v=XVBHishpew8> (vidéo YouTube : qu'est-ce que le RGPD ?)
- https://www.youtube.com/watch?v=3fuirT_PwDI (vidéo YouTube : le RGPD expliqué)
- <https://www.youtube.com/watch?v=PVaVIOJniSQ&t=6s> (vidéo YouTube : mes données, mon choix)
- https://cris.vub.be/files/27962258/arcades_teaching_handbook_final_EN.pdf (Université libre de Bruxelles (VUB) : Le manuel européen pour l'enseignement de la vie privée et de la protection des données dans les écoles)
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf (UK GOV : Data protection : a toolkit for schools)





- <https://www.gdpr.school/free-resources/> (sources utiles sur le RGPD pour les écoles)
- https://edpb.europa.eu/about-edpb/board/members_en (Liste des autorités nationales de protection des données)
- <https://ico.org.uk/> (site de l'autorité britannique de protection des données : beaucoup d'informations !)
- <https://en.mediawijs.be/poster-step-by-step-how-should-i-protect-my-privacy-on-social-media> (site web Mediawijs "Comment protéger ma vie privée sur les médias sociaux ?")
- https://www.youtube.com/results?search_query=internet+sécurité+conseils+pour+les+adolescents (vidéo YouTube avec des conseils de sécurité sur Internet pour les adolescents)
- <https://www.youtube.com/watch?v=yrln8nyVBLU> (YouTube : Safe Web Surfing : Top Tips for Kids and Teens Online)
- <https://mediawijs.be/nieuws/slag-gdpr-jouw-klas> (site web de Mediawijs sur l'utilisation du GDPR dans le cadre de vos cours en néerlandais)

Sources supplémentaires

- <https://d1afx9quaogywf.cloudfront.net/sites/default/files/Resources/School%20College%20Personal%20Data%20Advice%20and%20Guidance.pdf> (Informations pour les écoles afin de se conformer au GDPR)
- <https://www.youtube.com/watch?v=xtLR0Ey5-vo&t=76s> (vidéo YouTube contenant des informations permettant aux écoles de se conformer au RGPD)
- <https://www.youtube.com/watch?v=SpjpxspJNew&t=7s> (vidéo YouTube contenant des informations permettant aux écoles de se conformer au RGPD)





Points clés à retenir

La sensibilisation au RGPD est cruciale

Il est essentiel qu'à l'ère numérique d'aujourd'hui, les étudiants et les enseignants et tous les autres membres du personnel des établissements d'enseignement soient conscients du RGPD et de la législation sur la protection des données en général. Le montant personnel les données qui circulent en ligne sont énormes et ne feront que croître, c'est pourquoi chacun doit apprendre à gérer ses données personnelles et celles des autres de manière responsable.

Pourquoi le RGPD est-il important ? La valeur des données personnelles !

Nowadays, we all produce huge amounts of personal data on a daily basis, especially online (e.g. by posting pictures, videos or status updates on social media, but also by online shopping, reading an online newspaper or playing online games – this all generates data that can be linked to you). Some companies – besides collecting and processing personal data to deliver a specific service – aim to collect as much data as possible to effectively target you with advertising. Personal data thus has an important economic value to companies and organizations. Moreover, public authorities are interested in personal data as it can provide them new insights. But also people with malicious intentions such as hackers and identity thieves are out for your data. An uncontrolled use of personal data could consequently put private companies, hackers and public authorities in a position of power and put you in an undesirable situation.

Réfléchissez avant de partager

Réfléchissez toujours attentivement aux données personnelles que vous partagez avec qui et comment vous souhaitez présentez-vous dans les publications sur les réseaux sociaux (texte, images, vidéos). Il est important de penser à long terme ici parce que l'information pourrait flotter sur le World Wide Web pour toujours car il n'est pas facile de supprimer des informations sur Internet. Prenez soin de vos paramètres de confidentialité afin que les personnes que vous ne connaissez pas ne peut pas voir (une grande partie de) vos données personnelles. Même en exerçant le droit à l'effacement, vous aurez le plus probablement pas en mesure d'effacer toutes vos traces numériques.

Puis-je donner mon propre consentement pour le traitement de mes données personnelles ?

Il existe un âge légal pour que les enfants puissent consentir (ou non) eux-mêmes au traitement des données personnelles par les fournisseurs de services en ligne. Cette limite d'âge peut varier entre 13 et 16 ans en chaque État membre de l'UE. La transparence/l'information est essentielle L'un des grands principes qui sous-tendent le RGPD est le principe de transparence : les entreprises et les organisations doivent être claires sur le fait qu'elles traitent vos données personnelles, quelles données personnelles qu'ils traitent, pour quelles raisons et comment ils le font, pendant combien de temps, etc. Ce principe se traduit par le droit des personnes à être informées, ce qui devrait vous permettre de faire des choix éclairés sur votre données personnelles. De cette façon, le





RGPD veut rendre les individus responsables de ce qui arrive à leur vie personnelle Les données.

Comment savoir ce qu'une entreprise ou une organisation fait de mes données personnelles ?

La première chose à faire lorsque vous souhaitez savoir quelles sont les entreprises ou les organisations faire avec vos données personnelles est d'aller consulter la politique de confidentialité. Cette politique doit comporter un certain nombre d'éléments obligatoires. S'il semble qu'il manque quelque chose ou si quelque chose n'est pas clair, vous pouvez essayer de contacter l'entreprise ou les organisations pour plus de précisions.

Que faire si quelqu'un abuse de mes données sur les réseaux sociaux ?

Option 1 : contactez la personne/l'entreprise/l'organisation qui utilise vos données personnelles dans un manière illégale et leur demander de supprimer ou de corriger vos données personnelles.

Option 2 : contacter la plateforme de médias sociaux afin de demander la suppression ou la correction de vos données personnelles.

Option 3 : déposer une plainte auprès de votre autorité nationale de protection des données (voir leur site internet).

(Option 4 : aller au tribunal)





Infographies

Voir tout le matériel pédagogique + l'infographie ci-dessous.

Que faire lorsque quelqu'un utilise illégalement vos données personnelles sur les médias sociaux ?

1. Contactez la personne/société/organisation qui utilise vos données personnelles de manière illégale et demandez-lui de supprimer ou de corriger vos données personnelles.

2. Contactez la plateforme de médias sociaux afin de demander la suppression ou la correction de vos données personnelles.

3. Déposez une plainte auprès de votre **autorité nationale de protection des données** (voir son site web).





Plans d'activités avec les élèves

- Commencez le cours en demandant aux élèves s'ils savent ce que sont les données personnelles et pourquoi ils pensent qu'il est important de les protéger.
- Laissez les élèves vérifier leurs paramètres de confidentialité sur Facebook (ou un autre site de médias sociaux) : qui peut voir quel type d'informations vous concernant ? Ensuite, il peut y avoir une discussion entre les camarades de classe qui partagent les raisons pour lesquelles ils veulent que leurs paramètres soient d'une certaine manière ou s'ils souhaitent modifier leurs paramètres.
- Demandez aux élèves de rechercher le seuil d'âge pour donner valablement son consentement en vertu du RGPD dans votre pays. Cela peut se faire sur le site Web de votre autorité nationale de protection des données.
Voir : https://edpb.europa.eu/about-edpb/board/members_en.
- Après avoir reçu des informations sur le principe de transparence, l'un des principes centraux du RGPD, et sur le rôle des politiques de confidentialité à cet égard, les élèves peuvent inspecter la politique de confidentialité d'un site Web de médias sociaux de leur choix pour vérifier si toutes les informations obligatoires s'y trouvent. Ils peuvent ensuite en discuter entre eux.
- Après avoir expliqué aux élèves qu'ils ont certains droits en ce qui concerne le traitement de leurs données personnelles, ils pourraient déposer une "demande d'accès" auprès de Facebook (ou d'un autre site web de médias sociaux), pour voir quelles données personnelles Facebook détient à leur sujet. Voir : <https://www.facebook.com/help/contact/2032834846972583>.





Évaluation de l'activité

Vous pouvez facilement évaluer si les élèves ont compris les informations sur le RGPD en appliquant des questionnaires avec des questions courtes dont la réponse est vraie ou fausse, comme dans les exemples ci-dessous :

1. Une photo montrant une personne de dos, totalement méconnaissable, n'est jamais une donnée personnelle au sens du RGPD ? (**Faux** : la photo en tant que telle, sans aucune autre information, n'est pas une donnée à caractère personnel mais à partir du moment où quelqu'un y ajoute le nom, l'adresse ou le numéro de téléphone de cette personne, la photo devient une donnée à caractère personnel car elle est désormais liée à une personne spécifique)

2. La plupart des sites web et des applis que j'utilise traitent mes données personnelles. (**Vrai** : la finalité du traitement des données personnelles peut varier. Par exemple, habituellement, le traitement d'un nom et d'un mot de passe est nécessaire à des fins d'authentification. Souvent, les données personnelles telles que le sexe, l'âge, les intérêts sont traitées à des fins de marketing).

3. Le RGPD ne traite pas toutes les données personnelles de la même manière. (**Vrai** : la principale distinction faite dans le RGPD est entre les données personnelles "ordinaires" et les catégories spéciales de données personnelles (par exemple, la santé, l'orientation sexuelle, la religion). Ces dernières doivent être traitées avec plus de précaution en raison de leur nature sensible (le partage de ces données comporte un risque plus important car elles pourraient plus probablement entraîner des conséquences indésirables, telles que la discrimination, l'exclusion, etc.) et c'est pourquoi, en principe, le traitement de ces données est interdit. (Les données relatives aux infractions pénales et les données concernant les enfants sont également soumises à un régime spécial).

4. Une école publie les bulletins scolaires de chaque élève en ligne pour permettre aux parents de comparer les résultats de leur enfant avec ceux de ses camarades de classe. Cela est autorisé car c'est dans l'intérêt de l'enfant. (**Faux** : Ce n'est pas ainsi que cela fonctionne. Pour chaque traitement effectué, une entreprise ou une autre organisation - y compris une école -, doit se fonder sur une base légale valide déterminée dans le RGPD. Étant donné que cela pourrait potentiellement affecter négativement les enfants, la seule façon pour une école de le faire est d'obtenir le consentement de chaque enfant et/ou parent.

5. Lors du traitement de données à caractère personnel, le consentement de la personne dont





les données sont concernées est toujours requis. (**Faux** : le consentement n'est qu'une base légale parmi une liste limitée de bases légales sur lesquelles les entreprises et autres organisations peuvent s'appuyer pour justifier leurs activités de traitement (voir articles 6 et 9 du RGPD). Par conséquent, le consentement n'est pas toujours nécessaire. Pour chaque activité de traitement, vous devez toujours choisir une base légale pour le traitement, en fonction de celle qui est la plus adaptée à la situation.

6. Dans le passé, vous avez consenti à ce que votre photo soit publiée sur la page d'un média social d'une entreprise et vous n'aimez vraiment plus cette photo. Malheureusement, comme vous avez donné votre consentement à la publication de la photo dans le passé, vous ne pouvez rien y faire. (**Faux** : vous pouvez toujours retirer votre consentement, ce qui signifie que l'entreprise devra supprimer la photo).

7. Certains élèves ont été photographiés en classe et ont donné leur accord pour que cette photo soit utilisée dans le prospectus de l'école. Plus tard, l'école a décidé de partager cette brochure sur ses pages de médias sociaux. Cela est autorisé par le RGPD. (**Faux** : le consentement doit être donné d'une manière spécifique et ne peut pas être regroupé à des fins multiples. Cela signifie que l'école aurait dû obtenir un consentement distinct et explicite pour l'utilisation du prospectus sur ses canaux de médias sociaux).

8. L'objectif principal du RGPD est de restreindre la publicité en ligne. (**Faux** : dans la société numérisée d'aujourd'hui, où les données personnelles sont super précieuses, le RGPD vise à redonner aux citoyens le contrôle de leurs données personnelles en leur offrant une protection et des droits accrus + comme il s'applique directement dans toute l'UE, il harmonise les 27 lois différentes sur la protection des données).

9. Lorsque vous enregistrez sur votre téléphone la photo d'une autre personne que vous avez trouvée sur Instagram, uniquement pour montrer à votre coiffeur la coupe de cheveux que vous souhaitez, le RGPD ne s'applique pas. (**Vrai** : le RGPD ne s'applique pas aux activités personnelles et domestiques).

10. La publicité personnalisée/comportementale sur les médias sociaux n'est autorisée que si vous y avez consenti ? (**Vrai** : pour la publicité basée sur votre comportement de navigation, l'utilisation de cookies est nécessaire. Pour que les sites web puissent stocker ces cookies sur votre appareil, votre consentement préalable est nécessaire, sur la base des règles de la vie privée en ligne, et non du RGPD. En outre, les entreprises doivent toujours vous donner la possibilité de retirer ce consentement).









































