HORS NORME

Le RGPD, c'est quoi?

Introduction à la protection des données personnelles

À propos de

SOPHIE EVERARTS DE VELP

- **Sophie** est juriste, spécialisée en propriété intellectuelle, technologies de l'information, vie privée et e-commerce. Passionnée par ces matières depuis plusieurs années, Sophie est désormais consultante juridique chez Sedv Legal Services et Chercheuse en Droit du digital à l'Université de Namur.

Qu’est-ce que le RGPD?

Un nouveau règlement européen qui a vise à régler de manière uniforme la question de la vie privée

Le Règlement Général sur la Protection des Données (RGPD ou GDPR en anglais) est un règlement européen qui s’applique de manière uniforme dans tous les pays membres de l’UE.

L’objectif est de protéger les données personnelles des citoyens européens mais aussi de réglementer le transfert de ces données en dehors de l’UE.

L’UE souhaite redonner aux individus un contrôle sur leurs données.

Timeline

Début en 1995

Directive européenne 95/46

Adoption en avril 2016

Règlement européen

2016/679

25 mai 2018

Application effective

Nouvelle valeur marchande des données

Un service gratuit, ça n’existe pas. « Si c’est gratuit, c’est que c’est vous le produit ». La gratuité est la nouvelle tendance sur internet. Facebook, Snapchat, Instagram, Google Twitter, etc. fonctionnent tous sur ce modèle. L’objectif est de récolter toujours plus de données. en échange du service

Qui contrôle?

La Commission de la protection de la vie privée (CPVP) qui devient l'**Autorité de protection des données** (APD)

On passe d'un organe d'avis à un organe de contrôle et de sanctions

- Possibilité de donner des avertissements et d'infliger des amendes administratives

- Auparavant, pour sanctionner une entreprise, la CPVP était obligée d'entamer une procédure judiciaire, avec le risque que sa demande soit classée sans suite. Ex: affaire Facebook

Le secrétaire d'Etat De Backer "n'encaiss
pas la nouvelle politique de respect de l
vie privée de Google

27/10/16 à 12:44 - Mise à jou

Le secrétaire d'Etat en charge du respect de la vi ilippe De Backe
(Open Vld) "n'encaisse pas" le fait que le géant i ire n
mails, tienne à jour ce que nous visionnons su
informations à des publicitaires.

12
Fois partagé

Facebook gagne la bataille sur la vie privée en Belgique

MIS EN LIGNE LE 29/06/2016 À 18:40 L.CO AVEC BELGA

Retournement de situation dans le conflit qui oppose le réseau social et la Commission vie privée belge.

i7SUR7 INTERNET & JEUX EN LIGNE

BELGIQUE MONDE SPORTS SHOWBIZ PLUS 7S7

i7SUR7 INTERNET FACEBOOK

La commission de la vie privée et Facebook s'affrontent à nouveau

Recommander 0 Partager Tweet G+

Par: rédaction
12/10/17 - 16h50 Source: Belga

SAUVEGARDER

LIRE AUSSI


Le Tindstagramming: sortir par la porte et rentrer par la fenêtre


Une entreprise ne pourra plus surveiller les courriels privés de ses employés


À quel point votre patron peut-il vous surveiller?

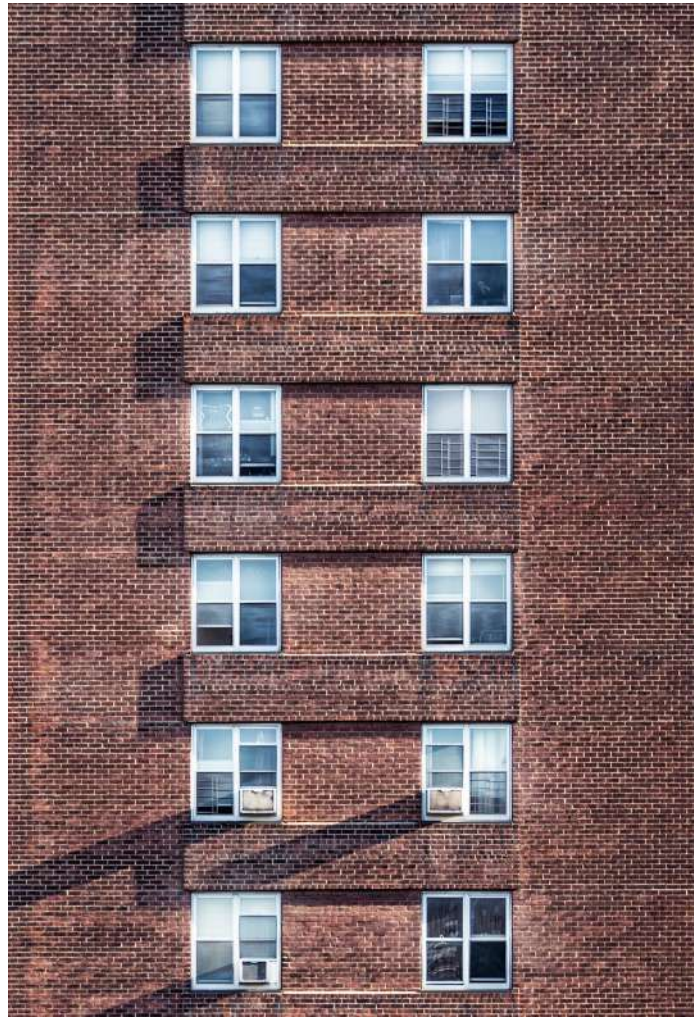
Plus d'infos sur Facebook , Vie privée sur Internet , Internet , Réseaux sociaux

La Commission vie privée examine la légalité du screening des festivaliers de Tomorrowland

Qui est concerné par le RGPD?

Toutes les entreprises qui traitent des données à caractère personnel de citoyens européens.
Peu importe où se situe l'entreprise, donc même si elle est située en dehors de l'UE.

Il s'agit d'un pas important dans la protection de la vie privée des particuliers. Auparavant, les géants du net comme Google, Amazon et Facebook échappaient à la législation européenne puisque leur établissement principal était situé dans la Silicon Valley.



C’est quoi une donnée à caractère personnel?

Toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée »).
Une donnée personnelle, c’est donc toute information qui permet d’identifier directement ou indirectement une personne physique.
Ex: nom, adresse postale, adresse IP, date de naissance, données de localisation, données bancaires, identifiants, plaque d’immatriculation, empreinte dentaire, etc.
>< contact@sedv-legal.com ou le compte en banque d’une entreprise.

C’est quoi traiter?

Toute opération ou tout ensemble d’opérations effectuées ou non à l’aide de procédés automatisés, telles que la collecte, l’enregistrement, l’organisation, la structuration, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l’interconnexion, la limitation, l’effacement ou la destruction

Ex: collecter, vendre ou utiliser des données , consulter des données ou stocker des données.

En bref, quasiment toute opération sur des données personnelles.

Responsable du traitement ou sous-traitant?

Le responsable du traitement est celui qui détermine quelles données vont être collectées, pour quelles finalités et par quels moyens.

Le sous-traitant est celui qui va traiter des données personnelles à la demande et pour le compte d'un responsable de traitement.

En tant qu'entreprise, vous avez généralement la double casquette.

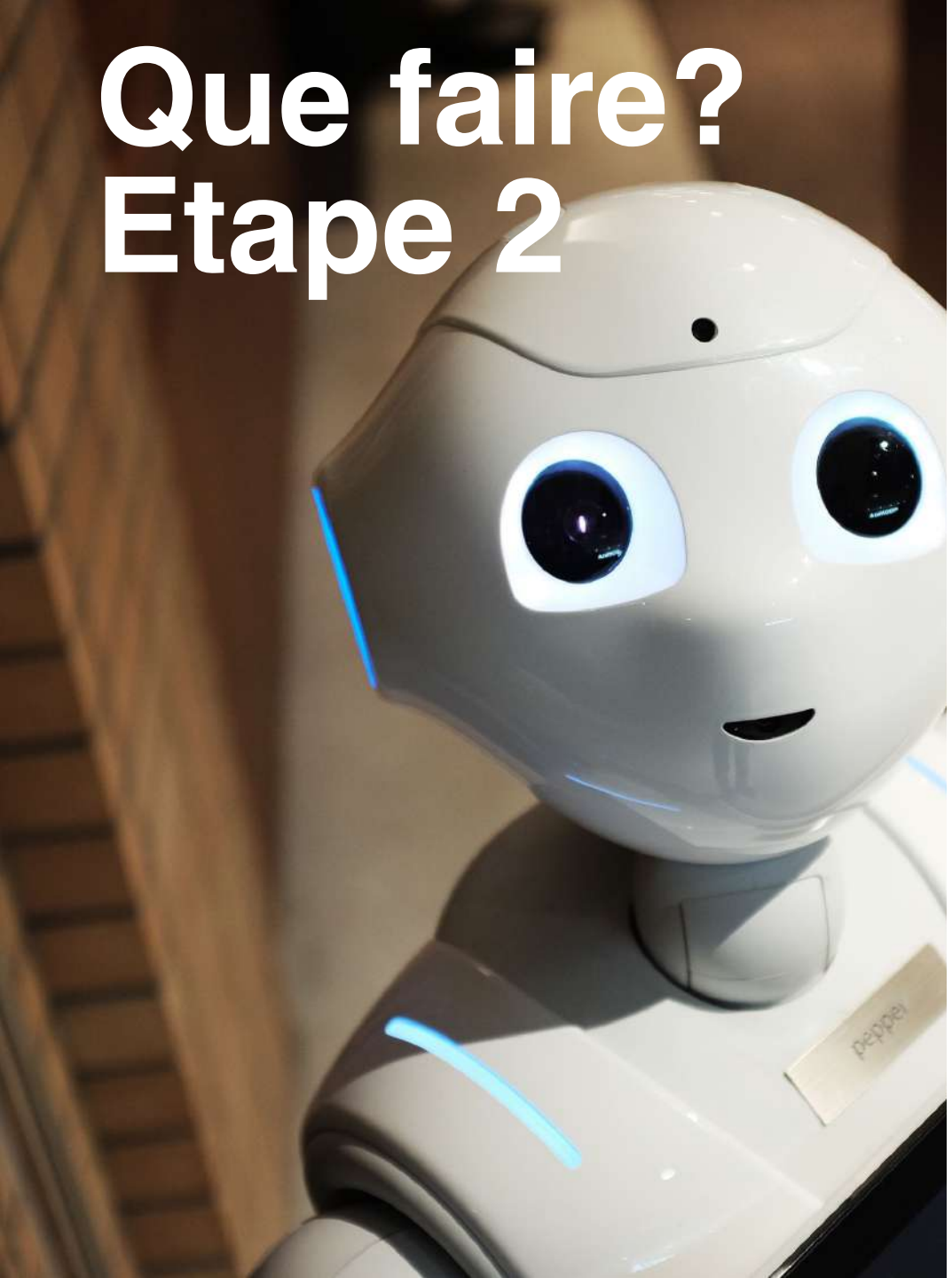
Que faire? Etape 1

Vos obligations en vertu du RGPD: respecter les principes généraux

Le RGPD repose sur six principes généraux que chaque traitement doit respecter. Ces principes doivent se refléter dans toutes les étapes que vous suivez et dans la manière dont vous effectuez chaque traitement.

Principes généraux

- Information et transparence
- Clair et précis
- Minimisation des données collectées
- Exactitude
- Intégrité et sécurité
- Durée de conservation limitée



Que faire? Etape 2

Trouver un fondement légal

1. Le consentement
2. L'exécution d'un contrat
3. Le respect d'une obligation légale
4. La sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique
5. L'exécution d'une mission d'intérêt public
6. L'intérêt légitime du responsable du traitement

Cas particulier

Les données sensibles

Données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat et les données génétiques, biométriques, relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle d'une personne physique.

Ces catégories de données personnelles bénéficient d'un régime de protection plus strict. Il est en principe interdit de traiter des données sensibles mais il existe un certain nombre d'exceptions, notamment le consentement (Ex: compagnies d'assurance).

La personne concernée a des droits sur ses données

Transparence et information renforcée

Chaque personne concernée doit avoir été informée du traitement de ses données dans un langage clair et compréhensible. Il y a un certain nombre d'informations à fournir, qui dépendent de si les données ont été recueillies directement ou non auprès de la personne concernée.

Cette obligation d'information prend souvent la forme d'une privacy policy (online ou papier).

Droit d’accès

« Droit de curiosité »

Est-ce que vous avez des données sur moi? Lesquelles?

Qu’est-ce que vous en faites? A qui vous les transmettez?

Combien de temps vous les conservez?

Quels sont mes droits?

Droit de rectification

La personne concernée a le droit d’exiger que ses données soient corrigées si elles sont fausses, incomplètes ou plus à jour.

Droit d’opposition

La personne concernée à la droit de s’opposer au traitement de ses données à tout moment.

Le droit d’opposition ne peut être exercé que dans certaines hypothèses, notamment pour s’opposer à la prospection commerciale et à l’envoi de newsletters.

Opposition = mettre fin au traitement

Droit à l’effacement (« droit à l’oubli »)

NEW !

La personne concernée a le droit d’obtenir l’effacement de ses données personnelles. Ce droit ne peut être exercé que dans 6 hypothèses.

Quand a-t-on un droit à l'oubli?

(1) Les données ne sont plus nécessaires au regard des finalités du traitement

(2) La personne concernée a retiré son consentement au traitement et il n'y a pas d'autre fondement légal

(3) La personne a exercé son droit d'opposition

(4) Les données ont fait l'objet d'un traitement illégal

(5) L'effacement des données est nécessaire au respect d'une obligation légale

(6) Les données ont été collectées dans le cadre d'une offre de services de la société de l'information adressée aux enfants

Droit à la portabilité

NEW !

La personne concernée peut demander au responsable du traitement de « récupérer » ses données. Ainsi, un particulier peut plus facilement changer de fournisseur. Ex: passer à un autre fournisseur de gaz et d'électricité ou à un autre opérateur télécom.

Quand faire valoir ce droit?

(1) Uniquement quand le traitement est automatisé et qu'il est fondé soit sur le consentement de la personne, soit sur un contrat.

(2) La personne concernée a aussi le droit de demander que ses données soient directement transmises au nouveau responsable du traitement, lorsque c'est techniquement possible.

Comment permettre l’exercice de ces droits?

- Privilégier un moyen technologique ou par mail
- Réponse dans les meilleurs délais et au plus tard 1 mois après réception de la demande

By design & by default

NEW !

Privacy by design: Garantir la protection des données dès la conception d’un nouveau produit ou service

Privacy by default: Limiter dès le départ le traitement des données à ce qui est strictement nécessaire (minimisation des données)

Délégué à la protection des données (DPO)

L’obligation de nommer un DPO est une nouveauté du RGPD. Elle s’applique aux responsables du traitement et aux sous-traitants. Ou du moins à certains d’entre eux. Vous êtes obligé de nommer un DPO si vous répondez « oui » à au moins une des questions suivantes.

1

AUTORITE

Vous êtes une autorité publique ou un organisme public

2

DONNEES SENSIBLES

Vous traitez principalement des données sensibles

3

SUIVI

Vous observez et suivez régulièrement le comportement de personnes physiques

Registre des activités de traitement

Plus d’obligation de déclaration préalable à l’autorité de protection des données

Par contre, l’entreprise doit tenir un registre des activités de traitement pour une transparence maximale.

Obligatoire pour les entreprises de 250 employés ou plus, et pour les plus petites entreprises qui traitent régulièrement des données ou qui traitent des données sensibles.

Mesures de sécurité adéquates

Vous devez garantir la sécurité des données en prenant des mesures techniques et organisationnelles.

Ces mesures doivent être proportionnelles au risque.

Au choix en fonction de l'état de la technique, des coûts de mise en oeuvre, de la nature et du volume des données, etc.

Violation des données (« data breach »)

Violation des mesures de sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisée de données à caractère personnel.

En cas de violation de données, le responsable du traitement doit en notifier la Commission Vie Privée dans les 72h après avoir constaté le problème, si celui-ci entraîne un risque pour les droits et libertés des personnes concernées. Si le délai est dépassé, le responsable du traitement devra justifier son retard.

Le sous-traitant qui constate une violation de données doit en avertir immédiatement le responsable du traitement.

Tout le monde en parle: les énormes amendes du RGPD.

Le RGPD permet maintenant à la Commission Vie Privée d'infliger des amendes administratives. Le montant maximal de l'amende peut s'élever jusqu'à 20 millions d'euros ou 4 % du CA mondial annuel de l'entreprise (par exemple si le consentement n'a pas été demandé ou si les règles de transfert hors UE n'ont pas été respectées). Il s'agit bien d'un montant maximal, dont l'objectif est surtout dissuasif. L'autorité de protection des données désire avant tout conscientiser les entreprises au respect de la vie privée.

Future règlementation? - e-privacy comme lex specialis du RGPD

Règlemente le secteur des communications électroniques. notamment l'envoi d'emails et l'utilisation des cookies.

RGPD: 2 ans de sanctions

- **En Allemagne**, la société de transport "Kolibri Image" a été condamnée à une amende de 5 000 € pour ne pas avoir conclu de contrat de sous-traitance.
- **Au Pays-Bas**: l'autorité néerlandaise de protection des données a infligé une amende de 600 000 € à "Uber" pour violation de l'obligation de signaler les violations de données.
- **Au Pays-Bas**: L'autorité néerlandaise de protection des données a infligé une amende de 48 000 € à "TGBBank", car elles n'avaient pas répondu à temps à la demande d'un client concernant l'accès à leurs données personnelles.
- **En Belgique**, l'autorité de protection des données belge (APD) a publié la première amende GDPR dans le pays. L'organe de protection de la vie privée a imposé une amende de 2 000 euros à un bourgmestre qui avait utilisé des adresses mail pour la diffusion de communications électorales, et ce, sans le consentement des personnes concernées.
- **En France**, la CNIL a infligé à Google une amende de 50 millions d'euros pour manquement à l'obligation de transparence.

Objectifs atteints ?

- Nombre de plaintes déposées en nette augmentation (+ de 100.000 en 2018 en Europe)
- Les sanctions et amendes ne suivent pas ce rythme
- De nombreuses entreprises ne sont pas encore en ordre
- Impact positif sur la protection des données et la vision des entreprises sur ces dernières
- **Conclusion**: l'intention était bonne mais l'objectif n'est clairement pas atteint après 2 ans.

Merci pour votre attention !

Avez-vous des questions ?