



GDPR & Données clients: 8 bonnes pratiques marketing



Elisabeth GUISSART
Avocat à la Cour

Fit4DataProtection – 14 mai 2018

PLAN

- 1 CARTOGRAPHIER**
- 2 RESPECTER GRANDS PRINCIPES**
- 3 SÉCURISER**
- 4 INFORMER**
- 5 S' ORGANISER FACE AUX DROITS DES PERSONNES**
- 6 OBTENIR LE CONSENTEMENT?**
- 7 ACHETER UNE BASE CLIENTS?**
- 8 PROFILER?**

1

CARTOGRAPHIER

REGISTRE OBJECTIFS



REGISTRE

FICHE: FICHER CLIENT

« photographie de la situation »

Données traitées

- Nom, prénom, téléphone, adresse, date de naissance?, coordonnées bancaires?, habitude d'achat?

Personnes concernées

- Clients

Finalité

- Gestion coordonnées clients, émission cartes fidélités, suivi/exécution commandes, envoi de newsletters, ...

Support/Localisation

- Logiciels utilisés / pays

Transfert

- Personnes ayant accès aux données (interne et externe), destinataires, sous-traitants

REGISTRE

FICHE: FICHER CLIENT

Questions à se poser

- Ai-je le droit d'effectuer le traitement? Sur quelle base a lieu de le traitement?
- Ai-je informé les clients? Comment? L'information est elle complète?
- Ai-je vraiment besoin de toutes les informations collectées?
- Combien de temps vais-je garder les données? Pourrai-je supprimer les données à fin du traitement?
- Les données sont-elles correctes et à jour?
- L'accès aux données est-il suffisamment limité?
- En cas de transfert hors EU, ai-je pris mes précautions?



2 RESPECTER GRANDS PRINCIPES

GRANDS PRINCIPES

4 PRINCIPES CLES

1 Finalité

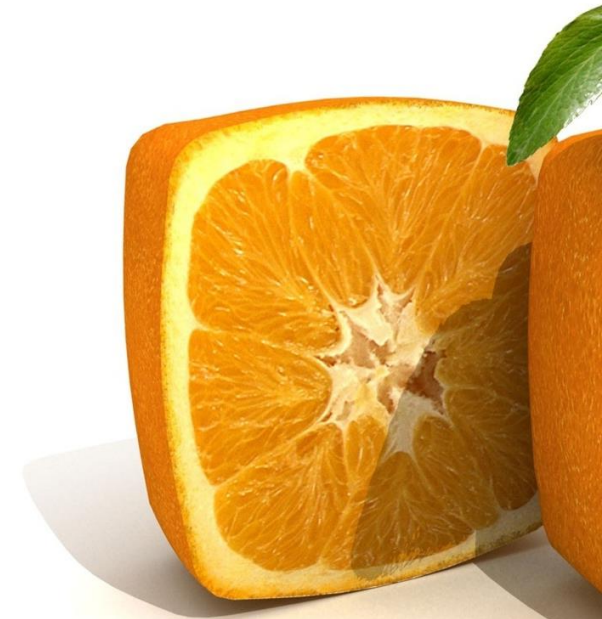
- traitement uniquement pour finalités déterminées, explicites, légitimes
- pas de traitement incompatible avec ces finalités

2 Pertinence

- données adéquates, pertinentes, non excessives / finalités
- données exactes et (si nécessaire) mises à jour

3 Rétention limitée

- données identifiant les personnes concernées conservées uniquement tant que nécessaires pour les finalités



GRANDS PRINCIPES

CLE DE VOUTE

PROPORTIONNALITE

- les moyens du traitement doivent être proportionnés à la finalité recherchée
- les actes de traitement doivent être nécessaires à atteindre la finalité recherchée



GRANDS PRINCIPES

FINALITÉ

La finalité est le but recherché par le responsable du traitement et qui justifie le traitement

- les finalités doivent être déterminées à l'avance
- les finalités doivent être légitimes
- toutes les finalités doivent être divulguées (transparence)
- les données ne doivent pas être traitées ultérieurement pour des **finalités incompatibles**

«compatible»: ce à quoi la personne concernée peut raisonnablement s'attendre



TRAITEMENT SECONDAIRE

consentement de toutes les personnes concernées
+ autorisation CNPD



GRANDS PRINCIPES

LÉGITIMITÉ

Un traitement «standard»
est légitime si...

TRAITEMENT «STANDARD»

DONNÉES SENSIBLES
SECTEUR DE LA SANTÉ
DONNÉES JUDICIAIRES

- obligation légale
- intérêt public important
- contrat/mesures pré-contractuelles avec la personne concernée
- intérêt légitime du responsable /droits et libertés de la personne
- intérêt vital
- consentement de la personne concernée

EMAILS
/SMS

GRANDS PRINCIPES

PERTINENCE

GDPR

+ minimisation des données

Les données doivent être:

- adéquates pertinentes et non excessives au regard de la finalité poursuivie
- régulièrement mises à jour



L'essentiel rien
que l'essentiel...

A screenshot of a web form for 'Fiskebar' (a restaurant in Antwerp). The form is titled 'Reservering > Gegevens > Controle' and shows a reservation for 'maandag 14 mei 2018 om 18:15 - 2 personen'. The 'Persoonlijke gegevens' section includes fields for 'Voornaam*', 'Achternaam*', 'E-mail*', 'Geboortedatum:' (with DD, MM, JJJJ dropdowns), and 'GSM:*' (with +32 and GSM dropdowns). There is an 'Aanmelden' link. Below this is a section 'Informatie voor Fiskebar' with a checkbox 'Schrijf mij in op de nieuwsbrief'. At the bottom are buttons for '< VORIGE' and 'VOLGENDE >'. A red circle with a question mark is drawn around the date field, with an arrow pointing to it from the right.

GRANDS PRINCIPES

RETENTION LIMITEE

Les données personnelles ne doivent pas être conservées de manière indéfinie

- Cas où la loi fixe une durée maximum (rare)
- Cas où la loi fixe une durée minimum
- Cas où la loi ne dit rien (principe)

Appréciation en fonction de la finalité

Penser en termes de cycle de vie !!

3 SECURISER

GDPR & SÉCURITÉ

EN AMONT

Data minimisation & privacy-by-design/by default

- les données les mieux protégées sont celles que l'on n'a plus, ou jamais eu...
- le principe de minimisation exige de ne collecter que les données indispensables pour la finalité
- *privacy-by-design* implique que les données devraient être détruites ou anonymisées/archivées/sécurisées systématiquement en fin de vie

The screenshot shows a registration form for 'Fiskebar' with the following fields:

- Persoonlijke gegevens** (Personal data) - [Aanmelden](#)
- Voornaam*: Voornaam
- Achternaam*: Achternaam
- E-mail*: E mail
- Geboortedatum: DD - MM - JJJJ (highlighted with a red arrow and question mark)
- GSM*: +32 GSM
- ☐ Reserveer voor iemand anders
- Informatie voor Fiskebar**
- ☐ Schrijf mij in op de nieuwsbrief

Navigation buttons: < VORIGE, VOLGENDE >



inscription à la newsletter

Bonjour,

Vous souhaitez recevoir notre newsletter OUI.sncf et être informé de nos promotions, complétez le formulaire suivant pour nous permettre de répondre au mieux à vos attentes :

E-mail* :

Confirmation de votre E-mail* :

Civilité :

Nom :

Prénom :

Date de naissance : / /



Pour être averti en temps réel de nos meilleures offres :

Mobile :

☐ Oui j'accepte de recevoir les meilleures offres sur mon mobile

Souhaitez-vous profiter des offres promotionnelles de nos partenaires commerciaux ?

☐ oui ☒ non



L'ensemble de votre inscription sera prise en compte lorsque vous aurez cliqué sur «Valider votre inscription»

* champs obligatoires

Valider votre inscription

GDPR & SÉCURITÉ

QUELLES MESURES DE SÉCURITÉ?

Familles de mesures de sécurité

- pseudonymiser les données, sauf justification
- moyens permettant de garantir confidentialité, intégrité, disponibilité et résilience constantes des systèmes
- moyens permettant de rétablir la disponibilité/accès en cas d'incident
- procédures de test/analyse et évaluation régulière de l'efficacité des mesures
- mesures afin de garantir que les employés ayant accès aux données ne les traitent pas, excepté sur instruction du responsable/de la loi

A noter: intégrité, disponibilité, résilience ne sont plus des «*nice to have*» et ne regardent pas que l'organisation...



GDPR & SÉCURITÉ

INCIDENTS DE SÉCURITÉ ET DIVULGATION DE DONNÉES

Data breach

- obligation d'informer:
 - CNPD sous 72h (ou plus tard sur justification)
 - personnes concernées sans délai, si leur vie privée est menacée
- exception si absence de risque pour les personnes concernées (ex. seules des données pseudonymisées ont été divulguées)
- incident doit être documenté (contexte factuel, effets, contre-mesures prises)
pour permettre à la CNPD de vérifier la conformité



GDPR & SÉCURITÉ

INCIDENTS DE SÉCURITÉ ET DIVULGATION DE DONNÉES

Data breaches & personnes concernées

- communication en langage clair/compréhensible
- doit inclure: nature de l'incident, coordonnées DPO, mesures prises ou proposées pour réduire les effets

Pas communication requise si:

- le responsable a appliqué des mesures aux données divulguées (pseudonymisation, cryptage) pour les rendre illisibles
- le responsable a pris des mesures correctives de manière à ce que le risque élevé potentiel ne se réalise pas
- impliquerait un effort disproportionné (communication publique requise dans ce cas)



4 INFORMER

DROITS DES PERSONNES CONCERNÉES

DROIT GÉNÉRAL À L'INFORMATION

Informations à communiquer

- identité du responsable
- finalités du traitement
- destinataires/catégories de destinataires
- caractère obligatoire/facultatif des questions, conséquences éventuelles défaut de réponse
- existence d'un droit d'accès/rectification

GDPR

+ coordonnées DPO
+ base juridique du traitement
+ intérêt légitime poursuivi
+ transfert vers pays tiers (niveau de protection local, mesures de sauvegarde)
+ durée ou critères de rétention
+ droit opposition
+ droit effacement
+ droit limitation
+ droit retrait consentement
+ droit réclamation/CNPD
+ données requises par la loi
+ contrat conditionné aux données
+ info sur décisions automatisées
+ info sur profilage
+ info logique sous-jacente & conséquences

PREUVE

**FORMER
STAFF**

DROITS DES PERSONNES CONCERNÉES

DROIT GÉNÉRAL À L'INFORMATION

Base de clients reçue d'un tiers?

- Catégorie données concernées
- Source de provenance des données
- Max. 1 mois après obtention MAIS
 - Au plus tard lors de la 1^{ère} communication (si objectif est de communiquer)
 - Au plus tard lors du 1^{er} transfert (si objectif est de transférer)



DROITS DES PERSONNES CONCERNÉES

DROIT GÉNÉRAL À L'INFORMATION

Caractéristiques

- Concision
- Transparence
- Précision
- Langage accessible, simple et clair
destinataires/catégories de destinataires



Support The Guardian

Subscribe

Find a job

Sign in

Search

News

Opinion

Sport

Culture

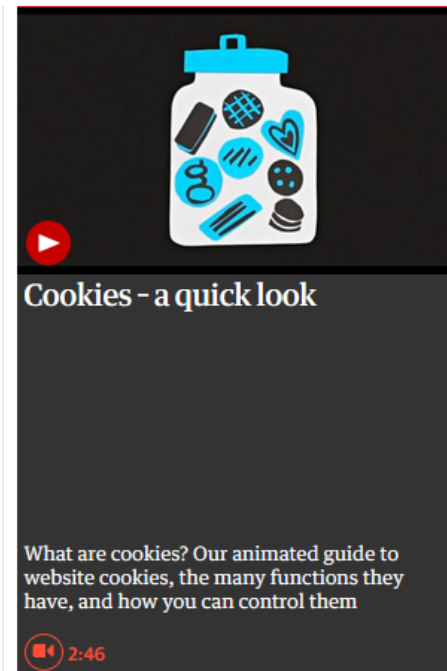
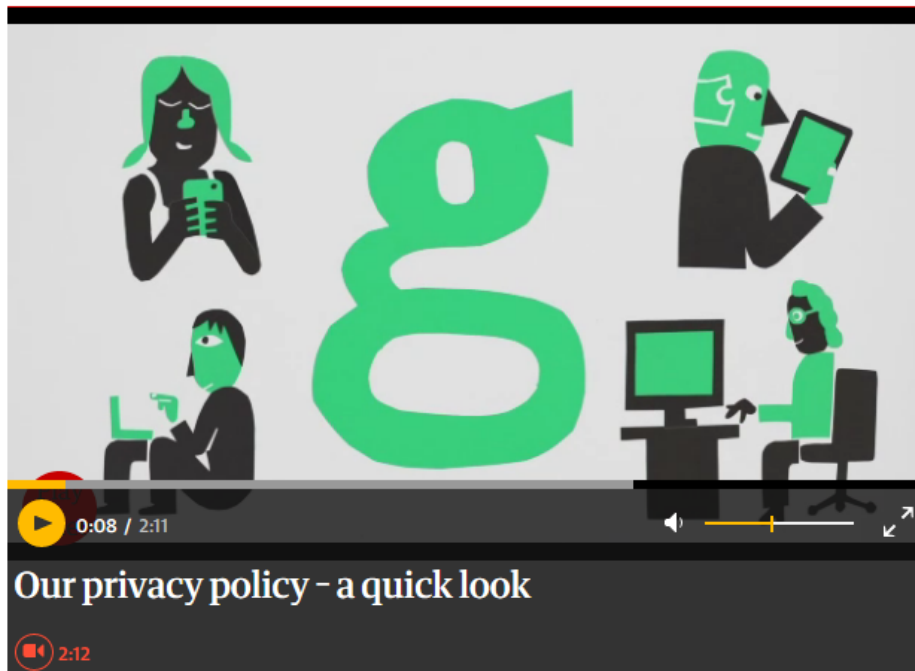
Lifestyle

More

The Guardian

International edition

Privacy



Tip us off

Share stories with the Guardian securely and confidentially



Further information



Read / Our privacy policy

Read / Our cookies policy

Infographic / Cookies on theguardian.com

Infographic / How to stay safe on the web

Hide

5

**S' ORGANISER FACE
AUX DROITS
PERSONNES
CONCERNES**

**RECTIFICATION
ACCES
OPPOSITION
EFFACEMENT
PORTABILITE
LIMITATION**



DROITS DES PERSONNES CONCERNÉES

DROIT D'ACCÈS

La personne concernée a normalement accès à toutes les informations la concernant

- accès illimité en théorie + copie
- exceptions (limitées) existent
- prudence recommandée avant tout refus de communiquer les données ou en cas de dissimulation de données
- communication logique qui sous-tend tout traitement avec décisions automatisées (y compris profilage)



DROITS DES PERSONNES CONCERNÉES

DROIT DE RECTIFICATION

Droit de faire rectifier les erreurs

- correction d'erreurs ou mise à jour uniquement
- ne pas confondre avec droit d'opposition
(qui est conditionnel)



DROITS DES PERSONNES CONCERNÉES

DROIT GÉNÉRAL D'OPPOSITION

Droit d'opposition

- conditionnel: pour des raisons prépondérantes et légitimes tenant à la situation particulière
- inconditionnel: traitement à des fins de prospection (+obligation d'informer de ce droit)
- inconditionnel: avant première communication de données à des tiers ou utilisation pour compte de tiers à des fins de prospection



DROITS DES PERSONNES CONCERNÉES

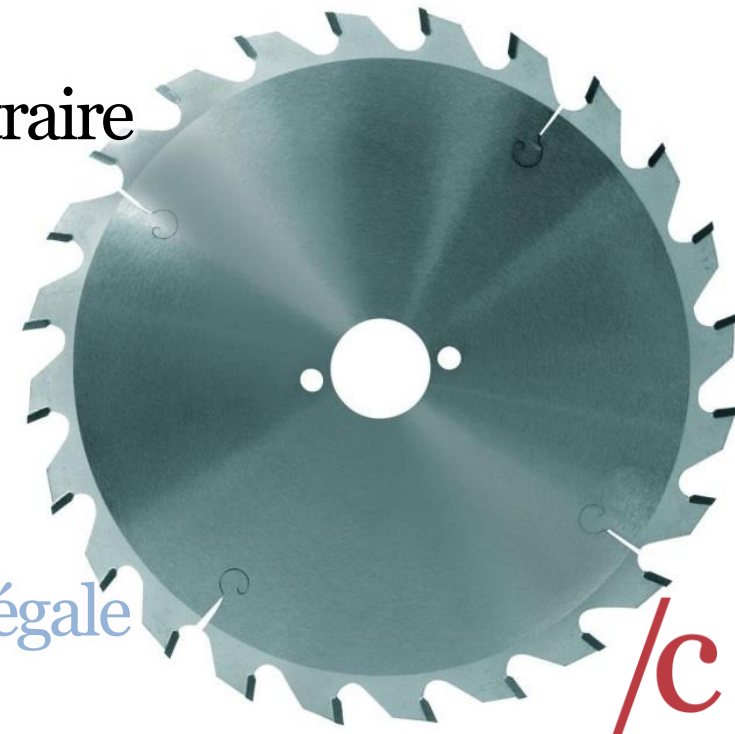
GDPR: DROIT À L'OUBLI

Droit à l'effacement

Sur demande de la personne concernée si:

- données plus nécessaires pour leur finalité
- retrait du consentement sans autre base de légitimité
- droit d'opposition + pas de motif légitime impérieux contraire
- opposition à prospection/profilage commercial
- données ont fait l'objet d'un traitement illicite
- effacement requis par la loi

Exceptions peu applicables données clients (sf obligation légale conservation)



6

OBTENIR
CONSENTEMENT?

PROSPECTION ÉLECTRONIQUE
COOKIES



GRANDS PRINCIPES

LÉGITIMITÉ

RAPPEL

Un traitement «standard»
est légitime si...

TRAITEMENT «STANDARD»

DONNÉES SENSIBLES
SECTEUR DE LA SANTÉ
DONNÉES JUDICIAIRES

- obligation légale
- intérêt public important
- contrat/mesures pré-contractuelles avec la personne concernée
- intérêt légitime du responsable /droits et libertés de la personne
- intérêt vital
- consentement de la personne concernée

EMAILS
/SMS

MARKETING & DONNEES PERSONNELLES

PROSPECTION ELECTRONIQUE (sms, mails)

Principe: *opt-in* (consentement en amont)

- consentement préalable à la réception d'emails publicitaires
- consentement peut être retiré à tout moment

Exception: *opt-out* (retrait en aval)

- uniquement pour les clients ayant donné leur adresse dans le cadre d'une vente
- pour des produits ou services analogues
- possibilité d'exercer son droit d'opposition (*opt-out*) de manière simple dans chaque email
- Envoi vers une adresse « pro » - B2B



EPRIVACY =



Echanges de données clients?

Consentement requis

/c



inscription à la newsletter

Bonjour,

Vous souhaitez recevoir notre newsletter OUI.sncf et être informé de nos promotions, complétez le formulaire suivant pour nous permettre de répondre au mieux à vos attentes :

E-mail* :

Confirmation de votre E-mail* :

Civilité :

Nom :


Prénom :

Date de naissance : / /

Pour être averti en temps réel de nos meilleures offres :

Mobile :

☐ Oui j'accepte de recevoir les meilleures offres sur mon mobile

 ☐ oui ☒ non

L'ensemble de votre inscription sera prise en compte lorsque vous aurez cliqué sur «Valider votre inscription»

* champs obligatoires

Valider votre inscription

Consentement – GDPR & ePrivacy

1 Libre

NON
NE PAS LIER
L'EXÉCUTION D'UN
SERVICE AU
CONSENTEMENT À UN
TRAITEMENT NON
NÉCESSAIRE POUR CE
SERVICE

2 Spécifique

NON
T&C
OUI
POUR CHAQUE TYPE DE
MARKETING
ÉLECTRONIQUE

3 Informé

4 Acte
positif

NON
INACTIVITÉ
SILENCE
CASE PRÉ COCHÉE

MARKETING & DONNEES PERSONNELLES

OBTENIR LE CONSENTEMENT?

EPRIVACY =

Dans certaines hypothèses uniquement

- Envoi mails/sms prospection produits différents
- Envoi mails/sms prospection à non clients
- Transfert à partenaires commerciaux (qui auront besoin du consentement)
- Décision individuelle automatisée
- Profilage (pas toujours)

Exemples formulations

OPT OUT

Si vous ne souhaitez pas recevoir de notre part des offres commerciales pour nos produits ou services analogues à ceux achetés par, merci de cocher cette case ☐

MAILS:

Pour ne plus recevoir nos messages, cliquez-ici (lien qui fonctionne)

SMS:

Renvoyez STOP par SMS

OPT IN

- Pour recevoir nos offres commerciales, cochez cette case ☐

- Pour recevoir les offres commerciales de nos partenaires, cochez cette case ☐

*- Je souhaite recevoir des offres commerciales par
Email ☐ sms ☐ téléphone ☐*



MARKETING & DONNEES PERSONNELLES

COOKIES & TRACEURS

Certains cookies ne requièrent pas de consentement préalable

- cookie utile au fonctionnement du site/appli
- cookie nécessaire à la fourniture du service

Ex.: "user-input cookies" ou "session-id cookies"
"multimedia player session cookies »; "user interface customization cookies"

Tous les autres cookies sont soumis à *opt-in*

- cookies liés aux opérations relatives à la publicité ciblée
- cookies des réseaux sociaux générés notamment par leurs boutons de partage lorsqu'ils collectent des données personnelles sans consentement des personnes concernées.
- certains cookies de mesure d'audience (voir les exemptions ci-après)



MARKETING & DONNEES PERSONNELLES

COOKIES DE MESURE D'AUDIENCE

Pas de consentement préalable si et seulement si:

- cookies non recoupés avec d'autres traitements (ex: fichiers clients ou statistiques de fréquentation d'autres sites)
- uniquement production de statistiques anonymes
- ne doit pas permettre le suivi de la navigation sur différents sites
- utilisation de l'adresse IP pour géolocaliser l'utilisateur ne doit pas permettre de déterminer sa rue

Dans les autres cas (+ fréquents): *opt-in*



MARKETING & DONNEES PERSONNELLES

COOKIES & CONSENTEMENT

Information du public

- des finalités précises des cookies utilisés
- de la possibilité et des moyens de s'opposer à ces cookies
- de manière précise et compréhensible
Ex: bandeau + renvoi à une page d'information détaillée

Consentement

- doit résulter d'une action positive
Ex: continuer la navigation / case à cocher
- ne peut résulter de la simple consultation de la page « en savoir plus »
- choix de l'internaute doit être respecté / preuve à conserver



Question de la durée ?

7 **ACHETER/
UNE BASE
CLIENTS?**

MARKETING & DONNEES PERSONNELLES

ACHETER UNE BASE CLIENTS?

POSSIBLE MAIS

- Loyauté / transparence en amont vis-à-vis de la personne concernée
- Obligation d'information – exigences additionnelles
- Prospection électronique: consentement requis (OPT-IN)
- Consentement suffisamment précis
- Attention à la « revente »

Prudence donc

- Vérifier ce qui a été communiqué au consommateur
- Vérifier quand le consentement a été obtenu
- Disposer de la preuve du consentement
- Acheter auprès de revendeurs fiables



8 PROFILER?

MARKETING & DONNEES PERSONNELLES

PROFILAGE

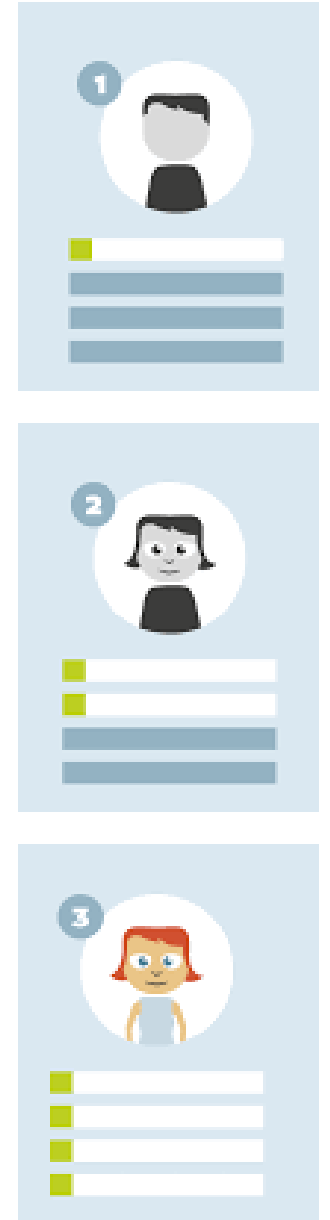
« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique »³

Caractéristiques

- Obtention d'infos et analyse de leurs caractéristiques en vue de les classer
- Intervention humaine non exclue
- Classification sur base âge, sexe, préférence = profilage
- Respect des principes de base (loyauté, légitimité, transparence)
- En général: fondé sur consentement ou intérêt légitime (attention à mise en balance intérêts - fonction granulosité profilage, étendue profilage, etc.



VIDÉOS
ICONES
CARTOONS
GRANULOSITÉ

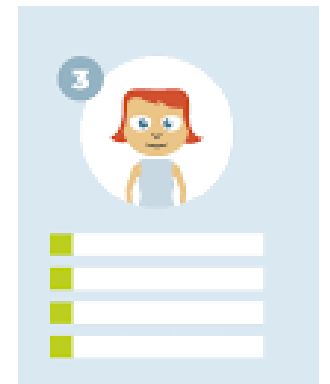
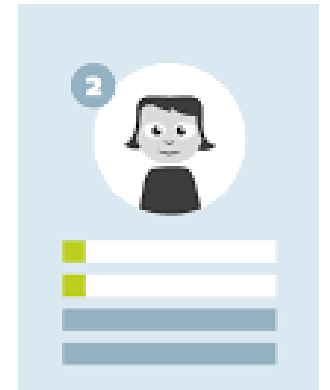
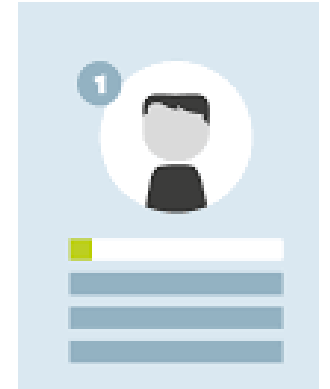


MARKETING & DONNEES PERSONNELLES

PROFILAGE

L'enrichissement d'une fiche de contact est un profilage

- pas illicite en soi: intérêt légitime du responsable de traitement
- sauf si fondement d'une décision automatisée ayant des effets juridiques ou affectant la personne de manière significative
- ou si données sensibles
- obligation d'information de la personne concernée
- toujours droit d'opposition de la personne concernée





Questions?

Elisabeth GUISSART
Avocat à la Cour
(+352) 28 80 90 10
elisabeth.guissart@claw.lu
24, rue Jean l'Aveugle L-1148 Luxembourg

