RGPD

Éric BERTHOMIER
eric.berthomier@free.fr

28 octobre 2023

Version 1.5 - Version Stagiaire

RGPD - Historique

- Entrée en application le 25 Mai 2018

RGPD - Historique

- Entrée en application le 25 Mai 2018
- Le règlement s'applique à toute entreprise, administration européenne et toute entité qui vise ou commercialise des biens ou des services au sein de l'Union Européenne.

RGPD - Historique

- Entrée en application le 25 Mai 2018
- Le règlement s'applique à toute entreprise, administration européenne et toute entité qui vise ou commercialise des biens ou des services au sein de l'Union Européenne.
- Le texte couvre 3 dimensions :

RGPD - Historique

- Entrée en application le 25 Mai 2018
- Le règlement s'applique à toute entreprise, administration européenne et toute entité qui vise ou commercialise des biens ou des services au sein de l'Union Européenne.
- Le texte couvre 3 dimensions :
  - Les données des collaborateurs

RGPD - Historique

- Entrée en application le 25 Mai 2018
- Le règlement s'applique à toute entreprise, administration européenne et toute entité qui vise ou commercialise des biens ou des services au sein de l'Union Européenne.
- Le texte couvre 3 dimensions :
  - Les données des collaborateurs
  - Les données des clients et prospects

RGPD - Historique

- Entrée en application le 25 Mai 2018
- Le règlement s'applique à toute entreprise, administration européenne et toute entité qui vise ou commercialise des biens ou des services au sein de l'Union Européenne.
- Le texte couvre 3 dimensions :
  - Les données des collaborateurs
  - Les données des clients et prospects
  - Toutes les autres données manipulées par l'établissement (sous-traitants, prestataires, visiteurs...)

Définition d'une donnée personnelle

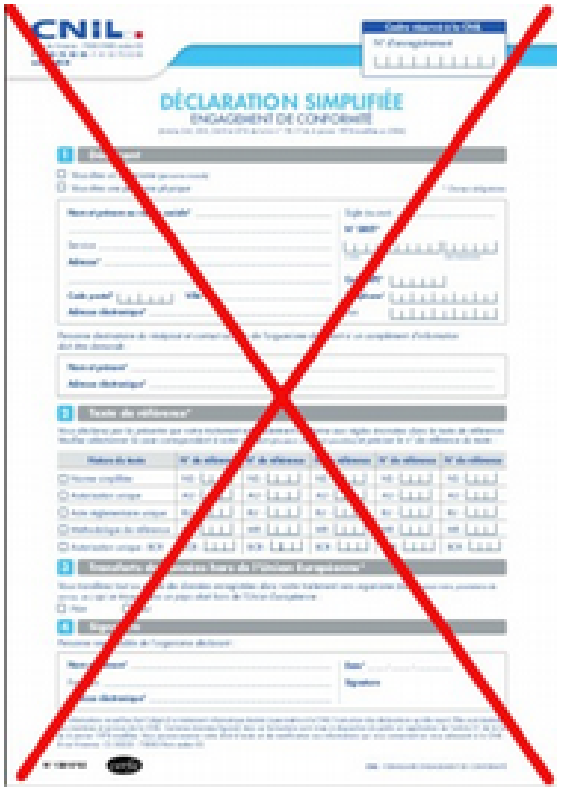
"Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à des éléments qui lui sont propres."

Définition d'une donnée personnelle

"Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à des éléments qui lui sont propres."

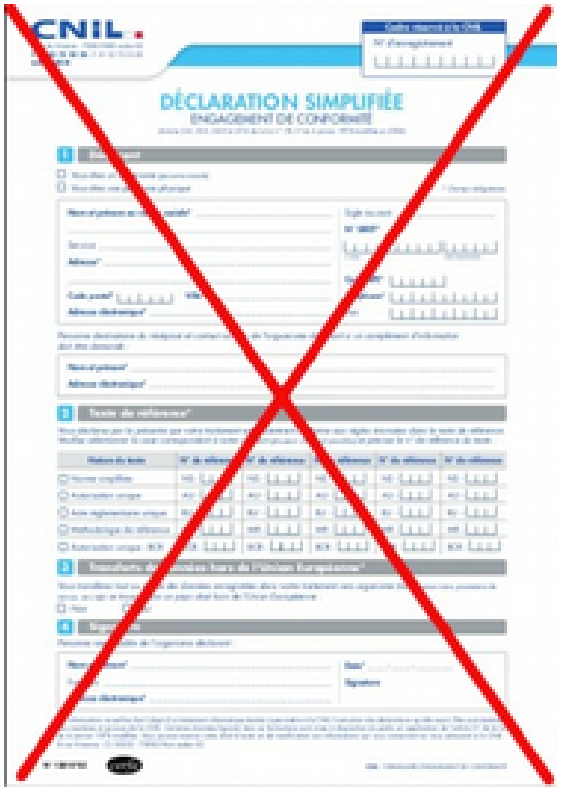
Donnez des exemples de données personnelles . . .

Avant / Après : le grand changement ?



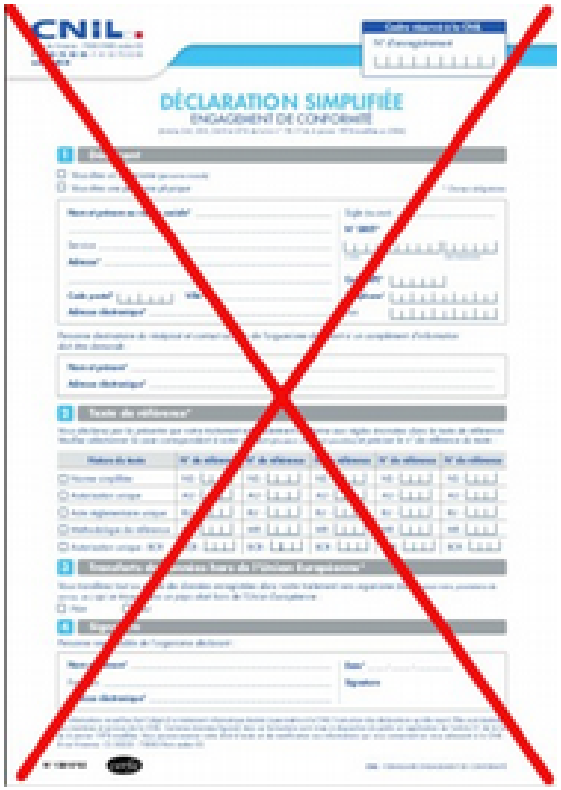
- Fin de la déclaration simplifiée

Avant / Après : le grand changement ?



- Fin de la déclaration simplifiée
- Naissance du PIA (Privacy Impact Assessment)

Avant / Après : le grand changement ?

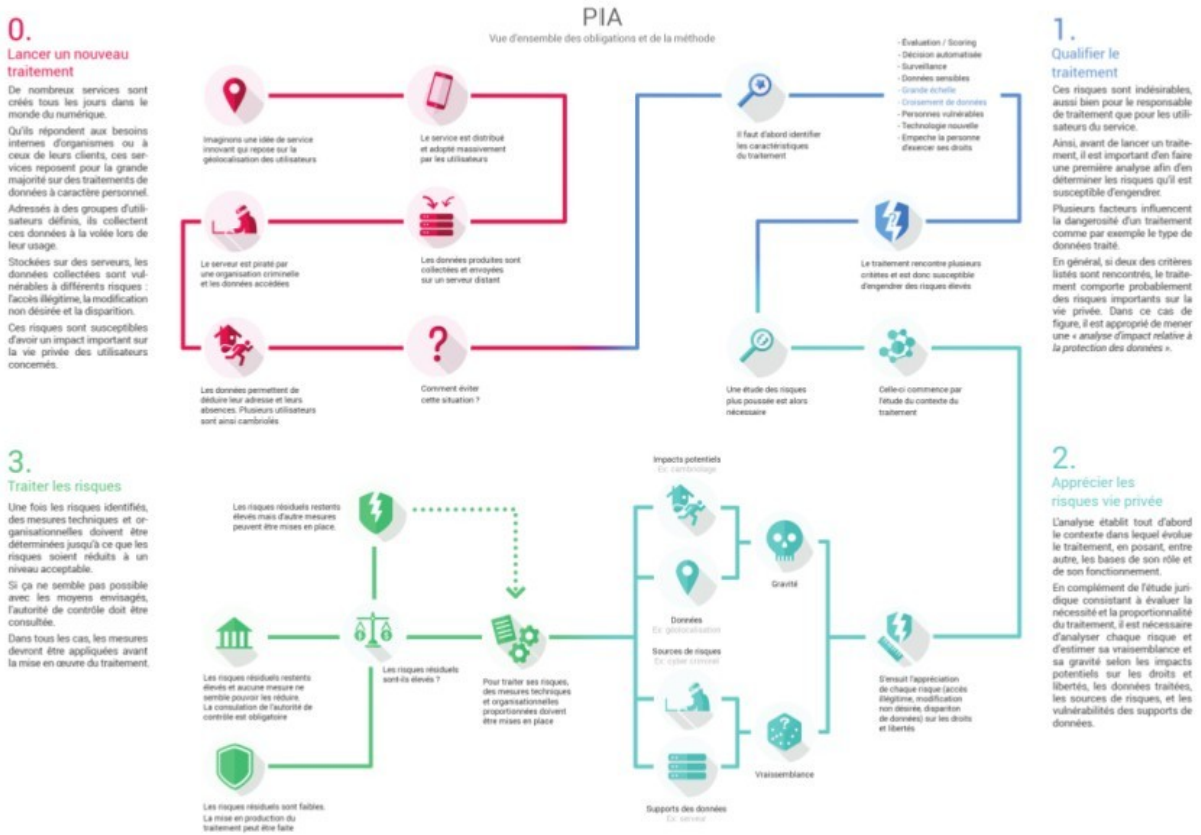


- Fin de la déclaration simplifiée
- Naissance du PIA (Privacy Impact Assessment)

pia | analyse d'impact sur la protection des données
privacy impact assessment

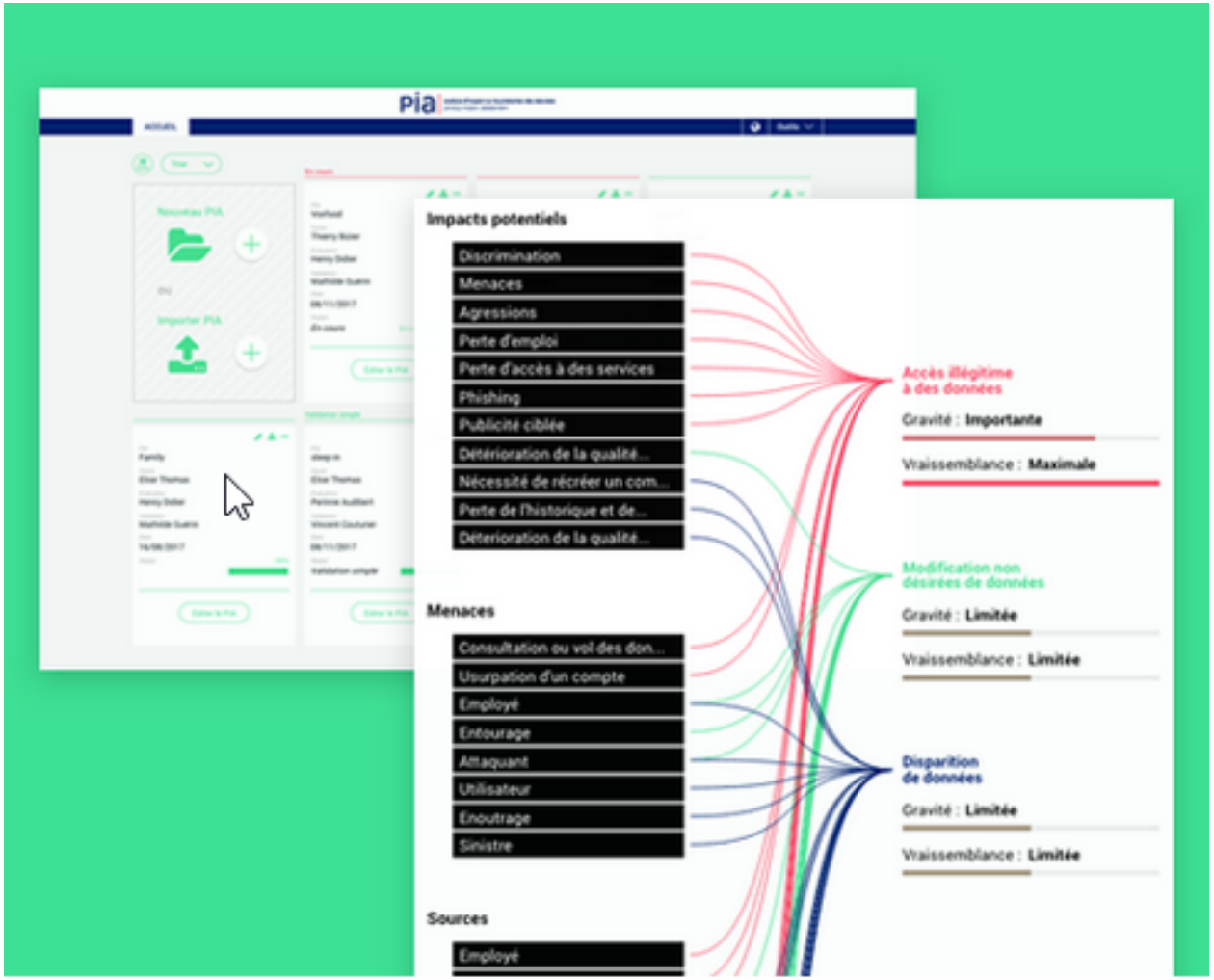
RGPD
RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

PIA Privacy Impact Assessment



Les mesures de protection devront être adoptées **avant** le traitement.

Mise à disposition d'un logiciel par la CNIL



Bien comprendre la conception antinomique des US

- Dans les pays anglo-saxons, on est propriétaire de ses données, on peut donc les céder **sans espoir de retour ni de contrôle**.

Bien comprendre la conception antinomique des US

- Dans les pays anglo-saxons, on est propriétaire de ses données, on peut donc les céder **sans espoir de retour ni de contrôle**.

- En France (et au niveau de l'Union Européenne), la protection des données personnelles fait partie des droits de la personnalité. On n'en est pas *"propriétaire"*, on ne peut donc s'en déposséder.

Bien comprendre la conception antinomique des US

- Dans les pays anglo-saxons, on est propriétaire de ses données, on peut donc les céder **sans espoir de retour ni de contrôle**.

- En France (et au niveau de l'Union Européenne), la protection des données personnelles fait partie des droits de la personnalité. On n'en est pas *"propriétaire"*, on ne peut donc s'en déposséder.

- D'où le terme de *"data subject"* (et non data owner).

Changement . . .

Le 10 juillet 2023, la Commission européenne a adopté une nouvelle décision dadéquation constatant que les États-Unis assurent un niveau de protection substantiellement équivalent à celui de l'Union européenne, permettant ainsi, **sous certaines conditions**, le transfert de données personnelles vers ce pays, sans exigences supplémentaires.

Changement . . .

Le 10 juillet 2023, la Commission européenne a adopté une nouvelle décision dadéquation constatant que les États-Unis assurent un niveau de protection substantiellement équivalent à celui de l'Union européenne, permettant ainsi, **sous certaines conditions**, le transfert de données personnelles vers ce pays, sans exigences supplémentaires.

Les transferts de données personnelles depuis l'Union européenne vers les organismes figurant sur une liste gérée et publiée par le ministère américain du commerce peuvent donc s'effectuer librement, sans encadrement spécifique par des "clauses contractuelles types" ou un autre instrument de transfert.

Source : CNIL

Étude de cas : je donne mon ADN . . .

Afin de connaître mes origines ethniques, je transmets mon ADN à une entreprise ...

- Quels en sont les incidences ?

Étude de cas : je donne mon ADN . . .

Afin de connaître mes origines ethniques, je transmets mon ADN à une entreprise ...

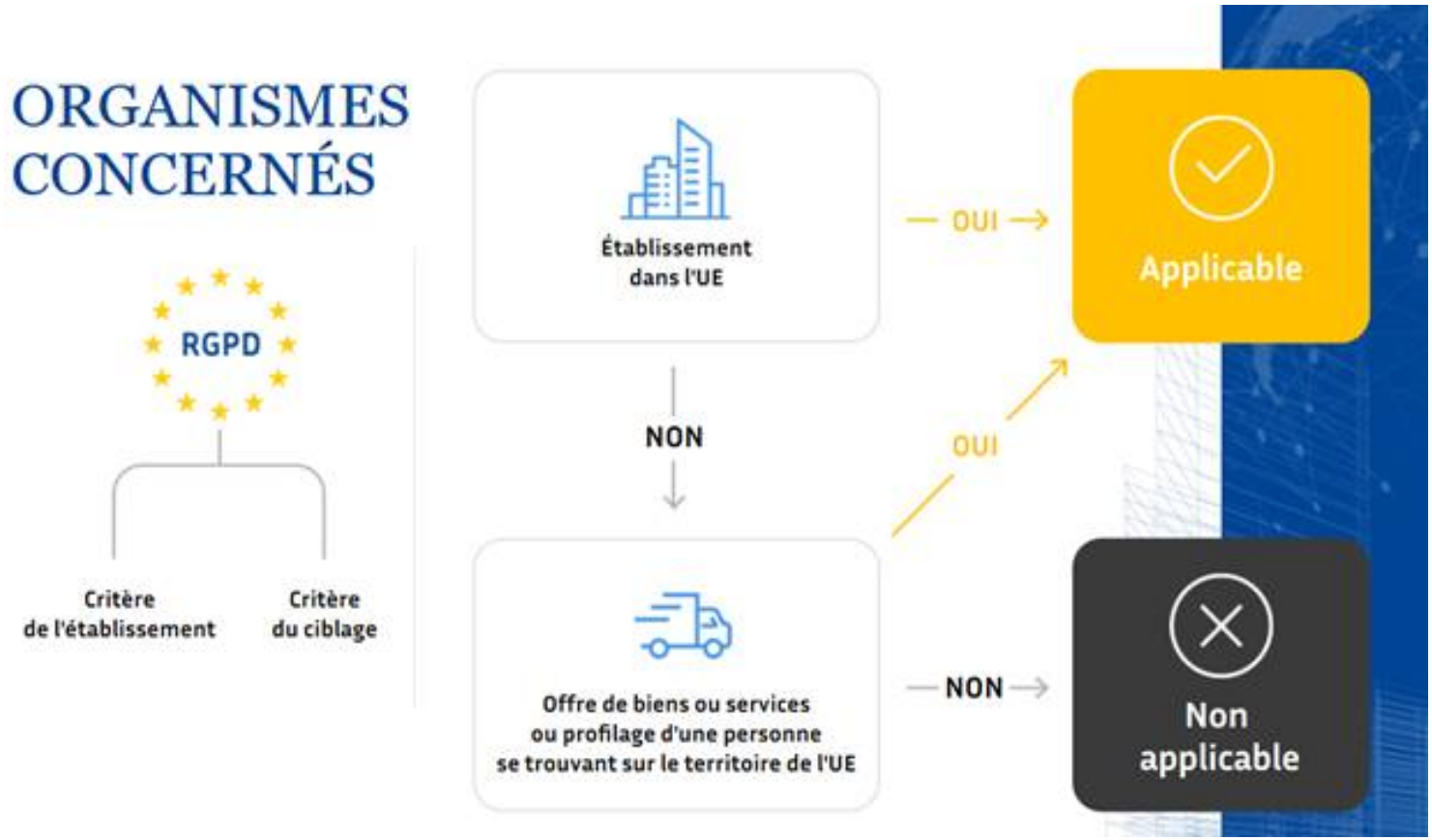
- Quels en sont les incidences ?
- Trouvez un site hébergé en Union Européenne permettant cette analyse .

Étude de cas : je donne mon ADN . . .

Afin de connaître mes origines ethniques, je transmets mon ADN à une entreprise ...

- Quels en sont les incidences ?
- Trouvez un site hébergé en Union Européenne permettant cette analyse .
- Conclure

Applicabilité



CIL / DPO / DPD

DPO : le référent

Le CIL, Correspondant Informatique et Libertés, se transforme en DPO (Data Protection Officer).
Il veille à la sécurité juridique et informatique de son organisme.

Info ou intox ?

" Le DPO est responsable pénalement et personnellement des non-conformités des traitements du responsable de traitement qui l'a nommé... "

Info ou intox ?

" Le DPO est responsable pénalement et personnellement des non-conformités des traitements du responsable de traitement qui l'a nommé... "

Comment dire... Non !

Info ou intox ?

" Le DPO est responsable pénalement et personnellement des non-conformités des traitements du responsable de traitement qui l'a nommé... "

Comment dire... Non !

En réalité le responsable de traitement reste... responsable !

Des principes existants renforcés(1/2).

Des principes existants renforcés(2/2).

1

CONTRÔLE DES DONNÉES

Renforcement des droits des citoyens européens en leur donnant plus de contrôle sur la mise à disposition des données personnelles

2

HARMONISATION

Cadre juridique unifié pour les organismes publics ou privés qui traitent des données personnelles

3

PREUVE

Demande de preuve de respect des exigences du Règlement

4

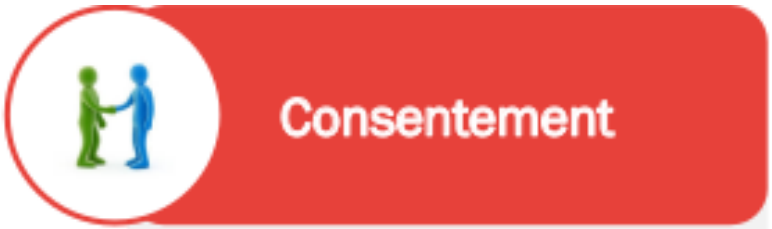
SANCTIONS

Plus d'obligations et de risques de sanctions

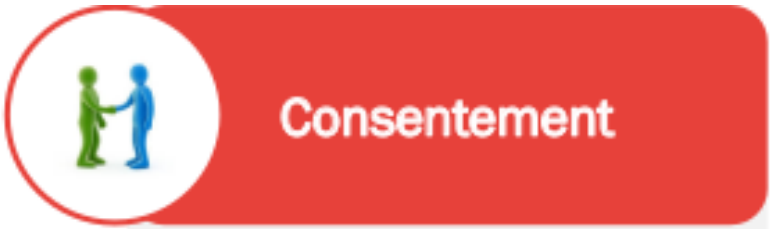
6 principes clés

En cas de non respect des dispositions du Règlement, les autorités de contrôle peuvent sanctionner l'entreprise à hauteur de 2 à 4% du chiffre d'affaires mondial du Groupe.
(Sanctions prévues à l'article 83 du Règlement.)

Consentement

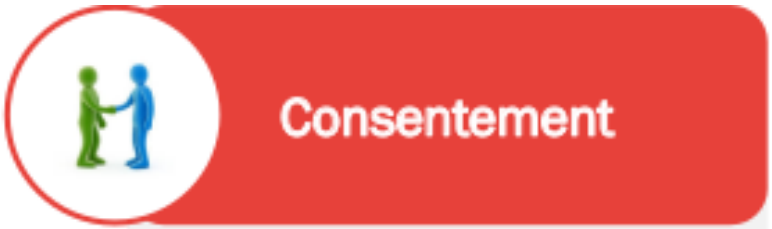


Consentement



Pas d'utilisation des données personnelles sans consentement

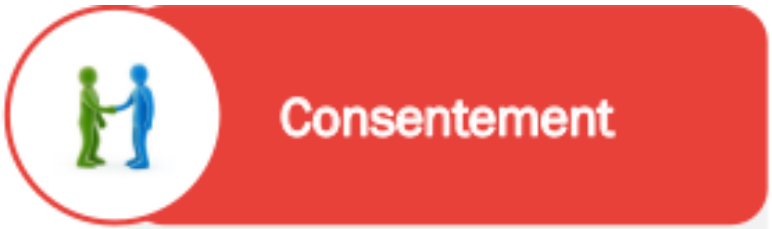
Consentement



Pas d'utilisation des données personnelles sans consentement

- L'utilisation des données personnelles doit faire l'objet d'un consentement **explicite**.

Consentement



Pas d'utilisation des données personnelles sans consentement

- L'utilisation des données personnelles doit faire l'objet d'un consentement **explicite**.
- L'établissement doit pouvoir prouver le consentement.

Transparence

Transparence

Les données à caractère personnel sont collectées uniquement pour une finalité donnée et prouvée

Protection à la conception des données

Protection à la conception des données

Protection à la conception des données

Le concept de "Privacy by design" ou protection des données dès la conception, vient garantir dans la durée la protection des données et complète.

Accès et portabilité

Accès et portabilité

Toute personne a le droit de disposer de ses données personnelles.

Accès et portabilité

Toute personne a le droit de disposer de ses données personnelles.

Les établissements sont tenus de donner accès aux données personnelles et de les rendre portables.

Rectification et effacement

Rectification et effacement

L'effacement ou le *"droit à l'oubli"* est garanti et prouvé.

Rectification et effacement

L'effacement ou le *"droit à l'oubli"* **est garanti et prouvé.** Les personnes concernées ont le droit de faire rectifier leurs données et d'en demander l'effacement.

Sous-traitants

Sous-traitants

Pas d'utilisation des données personnelles sans consentement.

Sous-traitants

Pas d'utilisation des données personnelles sans consentement.

- L'utilisation des données personnelles doit faire l'objet d'un consentement explicite.

Sous-traitants

Pas d'utilisation des données personnelles sans consentement.

- L'utilisation des données personnelles doit faire l'objet d'un consentement explicite.
- L'établissement doit pouvoir prouver le consentement

Obligation d'informer

easyJet

Avis d'incident de cybersécurité - soyez attentif aux e-mails malveillants de type phishing

easyJet

Comme vous le savez probablement, le 19 mai 2020, nous avons annoncé que nous avons été la cible d'une attaque hautement sophistiquée. Dès que nous avons eu connaissance de l'incident, nous avons immédiatement pris des mesures pour gérer et répondre à l'attaque, tout en fermant l'accès non autorisé. Nous avons engagé de grands experts forensiques pour enquêter sur la question et avons également informé le Centre National de Cybersécurité anglais ainsi que le Bureau du Commissaire à l'Information (ICO).

Notre enquête a révélé que votre nom, votre adresse électronique et vos coordonnées de voyage pour les réservations de vols

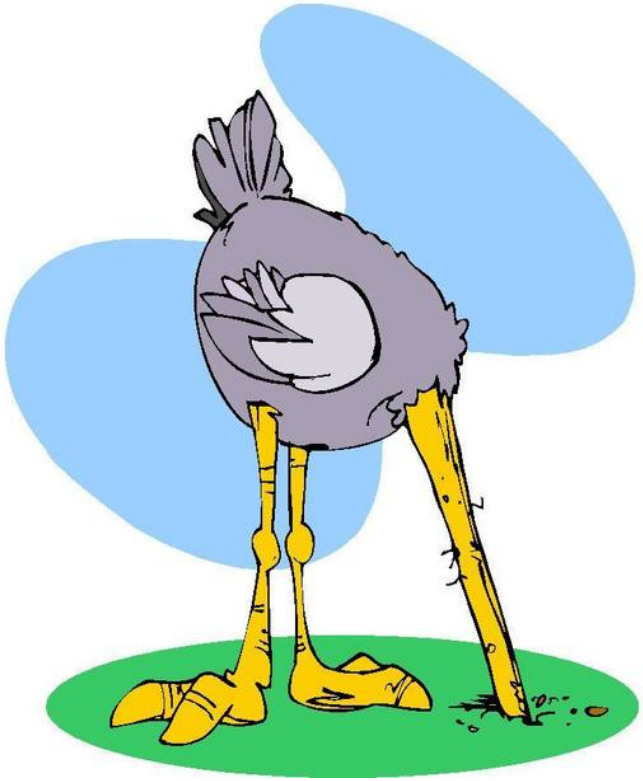
easyJet

Comme vous le savez probablement, le 19 mai 2020, nous avons annoncé que nous avons été la cible d'une attaque hautement sophistiquée. Dès que nous avons eu connaissance de l'incident, nous avons immédiatement pris des mesures pour gérer et répondre à l'attaque, tout en fermant l'accès non autorisé. Nous avons engagé de grands experts forensiques pour enquêter sur la question et avons également informé le Centre National de Cybersécurité anglais ainsi que le Bureau du Commissaire à l'Information (ICO).

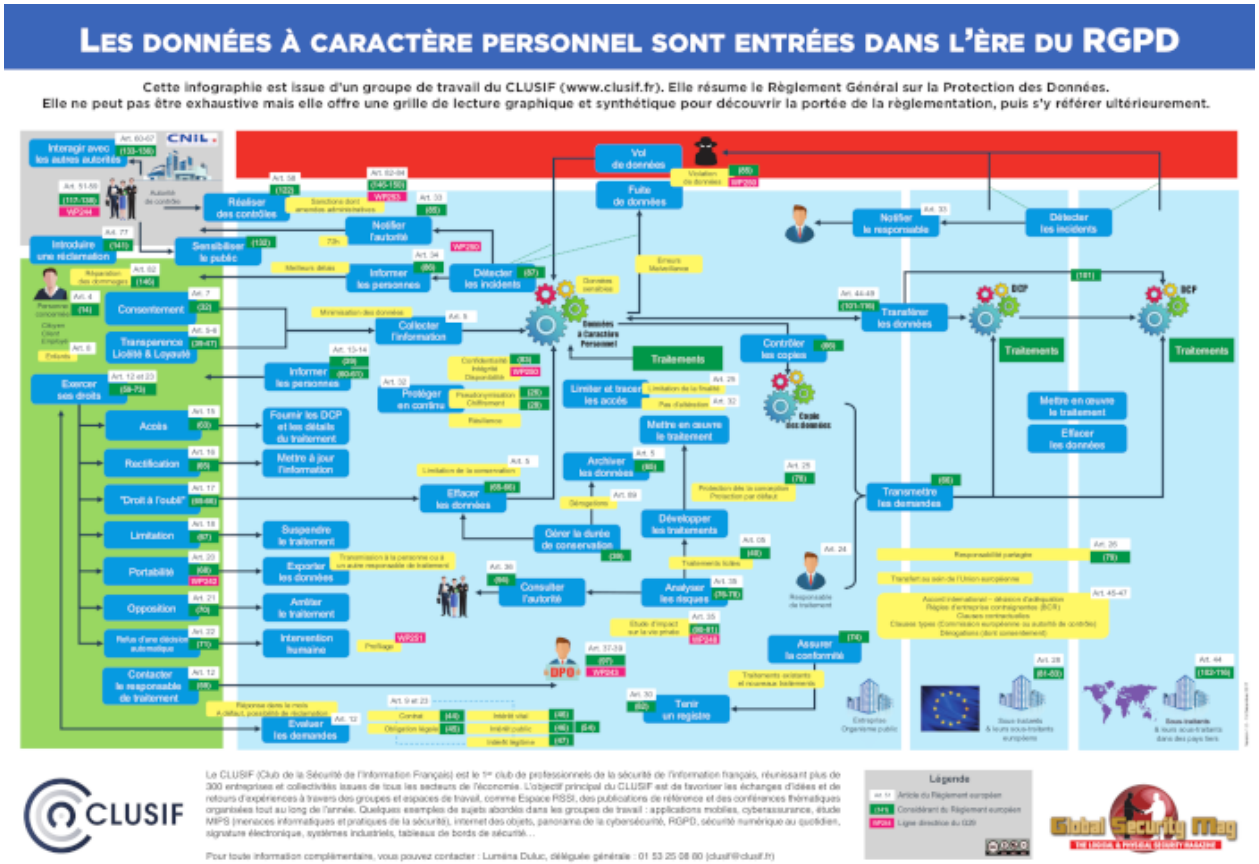
Notre enquête a révélé que votre nom, votre adresse électronique et vos coordonnées de voyage pour les réservations de vols

ZDNet - easyJet : action collective pour un montant de plus de 20 milliards d'euros pour vol de données contre la compagnie aérienne . . .

Vol de données ?



Législation



Côté pénal - Articles 226-16 à 226-24

Infraction	Texte	Peines
Non-respect des formalités préalables	Articles 226-16 du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Non-respect de l'article 34 de la loi Informatique et Libertés relatif à l'obligation de sécurité	Articles 226-17 et 226-17-1 du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Détournement de la finalité des données personnelles	Article 226-21 du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Procéder à un transfert de données transfrontières contrevenant aux mesures prises par la Commission des Communautés européennes ou à l'article 70 de la loi Informatique et Libertés	Article 226-22-1 du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Absence d'information des personnes concernées	Article R. 625-10 du Code pénal	1.500 euros d'amende par infraction constatée
Non-respect des droits des personnes	Article R. 625-11 du Code pénal	1.500 euros d'amende par infraction constatée