Conférences #ParisWeb

5 octobre 2017

PARIS WEB

Souriez (?) #GDPR, #PrivacyByDesign, #PrivacyByDefault deviennent réalité !

@slebarque

https://www.linkedin.com/in/stephanelebarque/

Stéphane Lebarque

https://www.niji.fr/

#Signification et #Contexte GDPR/RGPD

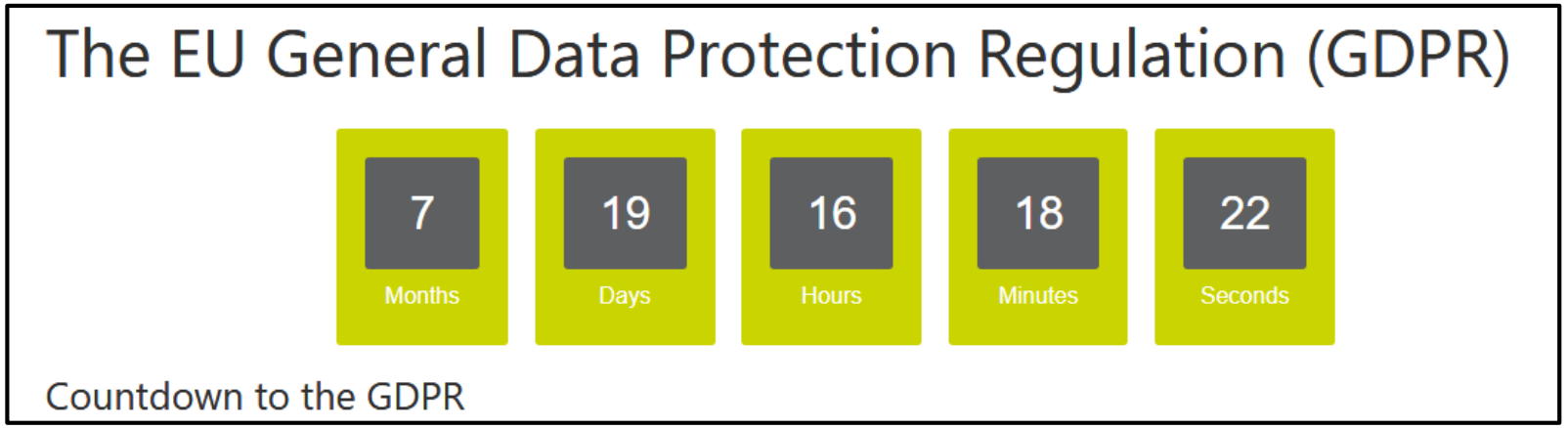
GDPR = **G**eneral **D**ata **P**rotection **R**egulation

RGPD = **R**èglement **G**énéral sur la **P**rotection des **D**onnées

CONTEXTE : 99 articles qui instaurent dans l'ensemble des pays de l'Union Européenne, les principes à appliquer par tous les acteurs (responsables de traitement et sous-traitants) qui détiennent, traitent des données à caractère personnel de citoyens européens. Et peu importe que ce traitement ait lieu ou non dans l'Union Européenne.

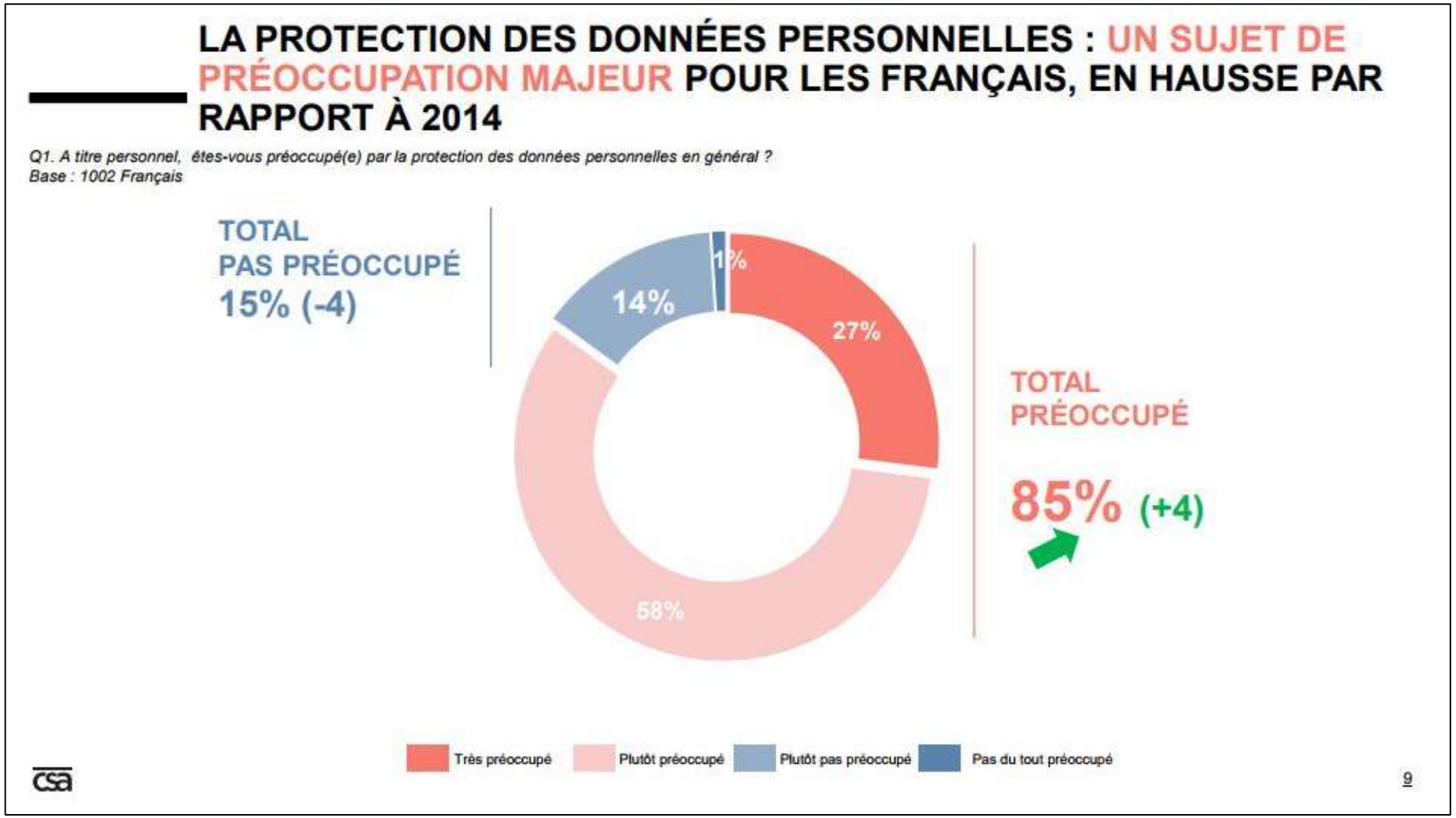
DATES :

- **24 mai 2016 :** entrée en vigueur
- **25 mai 2018 :** date limite de mise en conformité



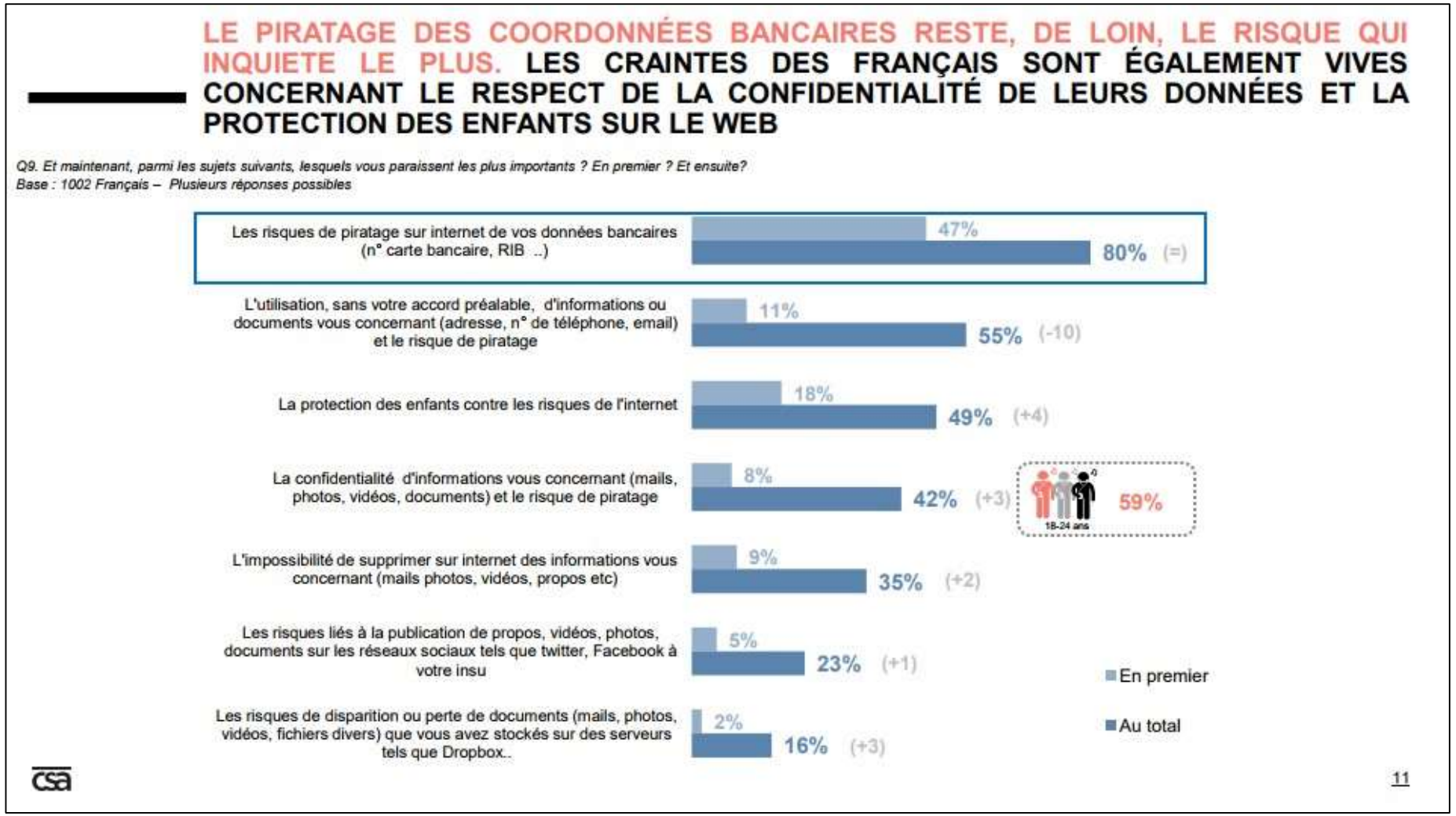
Source : https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

#Contexte : la protection des données personnelles, un sujet de préoccupation majeur pour les Français en 2017, en hausse par rapport à 2014 (Source : Enquête CSA publiée en Septembre 2017)



Source : https://www.csa.eu/media/1667/1700780-csa-protection-des-donnees-personnelles.pdf

#Contexte : la protection des données personnelles, un sujet de préoccupation majeur pour les Français en 2017, en hausse par rapport à 2014 (Source : Enquête CSA publiée en Septembre 2017)



Source : https://www.csa.eu/media/1667/1700780-csa-protection-des-donnees-personnelles.pdf

Objectif du règlement GDPR ?

« Si la data est l'or noir du XXIème siècle, la confiance en est la nouvelle monnaie : ainsi le GDPR vise à instaurer le cadre de cette confiance. »

Objectif global du GDPR => Redonner aux citoyens le contrôle de leurs données à caractère personnel, tout en simplifiant l'environnement réglementaire des entreprises !

Définition : Données à caractère personnel

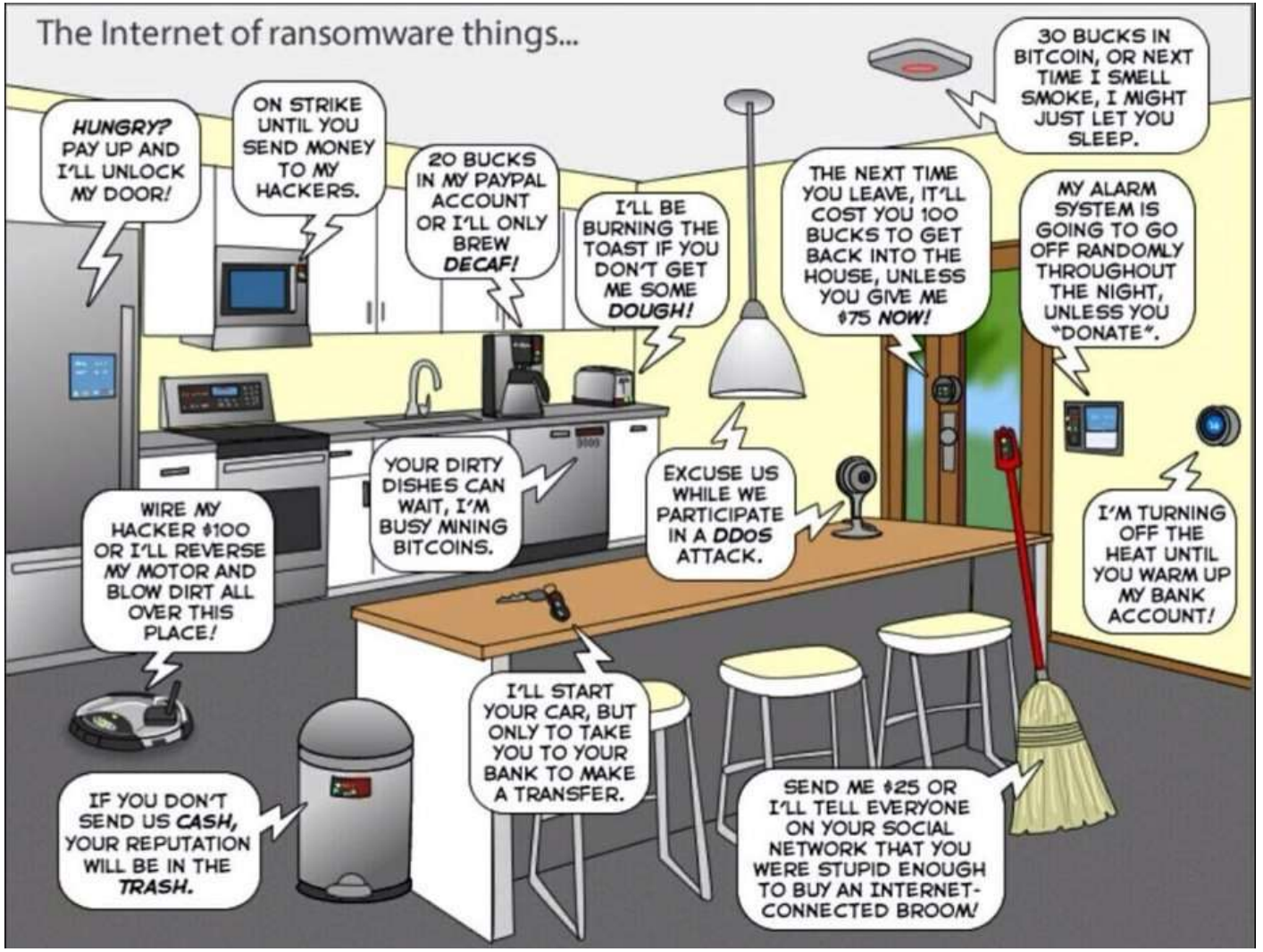
« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique **qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; »**

Exemples : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, un identifiant de connexion informatique, un enregistrement vocal, une adresse IP etc

Source : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4

Principe : #PrivacyByDesign

Dès le début de la conception de services, d'outils, d'objets connectés… il faut prendre en considération le respect de la vie privée, la protection des données en les sécurisant, en documentant les mesures techniques et opérationnelles mises en œuvre…



Source : https://twitter.com/MarksLarks/status/863293125422444544

Principe : #PrivacyByDefault

Mettre en œuvre les **mesures techniques** et **organisationnelles** appropriées **pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.** Cela s'applique à **la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité**.

Source : https://yamadonkey.wordpress.com/2017/04/10/choose-your-privacy-setting/

Plus de droits pour vos données à caractère personnel et concrètement 1/6

Des données à emporter !

Je peux récupérer les données que j'ai communiquées à une plate-forme et les transmettre à une autre (réseau social, fournisseur d'accès à internet, banques, etc.)

Source : https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees
Illustration : Martin Vidberg

Plus de droits pour vos données à caractère personnel et concrètement 2/6

Plus de transparence

Je bénéficie de plus de lisibilité sur ce qui est fait de mes données et j'exerce mes droits plus facilement (droit d'accès, droit de rectification,…).

Source : https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees
Illustration : Martin Vidberg

Plus de droits pour vos données à caractère personnel et concrètement 3/6

Protection des mineurs

Les services en ligne doivent obtenir le consentement des parents des mineurs de moins de 16 ans avant leur inscription.

Source : https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees
Illustration : Martin Vidberg

Plus de droits pour vos données à caractère personnel et concrètement 4/6

Guichet unique

En cas de problème, je m'adresse à l'autorité de protection des données de mon pays, quelque soit le lieu d'implantation de l'entreprise qui traite mes données.

Source : https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees
Illustration : Martin Vidberg

Plus de droits pour vos données à caractère personnel et concrètement 5/6

Consécration du droit à l'oubli

Je peux demander à ce qu'un lien soit déréférencé d'un moteur de recherche ou qu'une information soit supprimée s'ils portent atteinte à ma vie privée.

Source : https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees
Illustration : Martin Vidberg

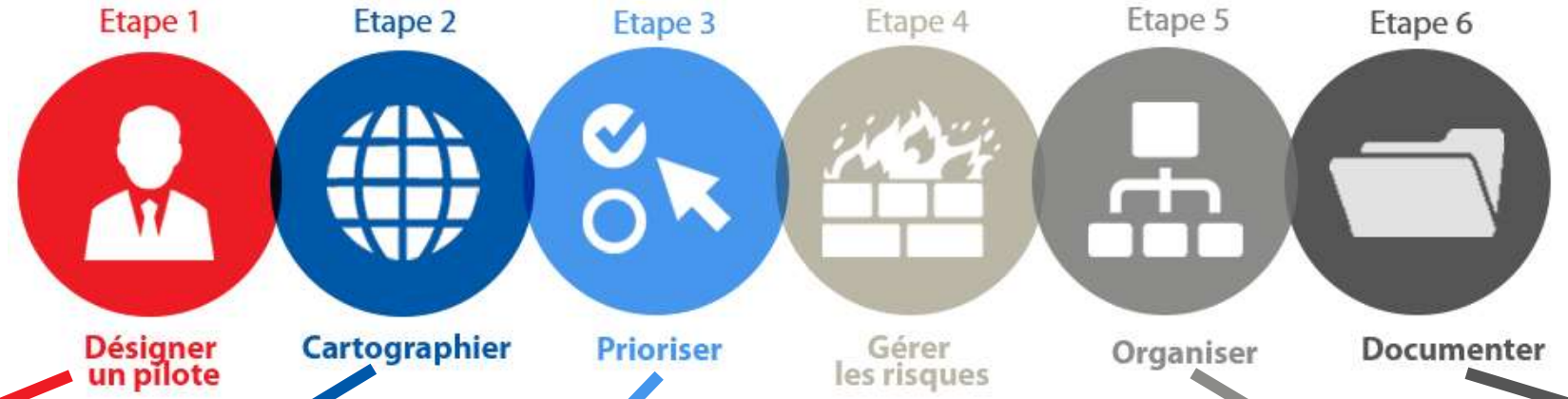
Plus de droits pour vos données à caractère personnel et concrètement 6/6

Sanctions renforcées

En cas de violation de mes droits, l'entreprise responsable encourt une sanction pouvant s'élever à 4% de son chiffre d'affaires mondial ou jusqu'à 20 millions d'euros !

Source : https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees
Illustration : Martin Vidberg

#Méthodologie CNIL de mise en conformité en 6 étapes



Le délégué à la protection des données (DPO =Data Protection Officer) = « chef d'orchestre » en charge
- d'informer et de conseiller
- de contrôler le respect du règlement
- de conseiller l'organisme
- de coopérer avec l'autorité de contrôle

Pour établir un registre des différents traitements de données personnelles, des catégories de données, des objectifs poursuivis, des acteurs (internes ou externes), des flux

Prioriser ces actions au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées.
- Révisez vos mentions d'information
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations,

Mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA) si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées

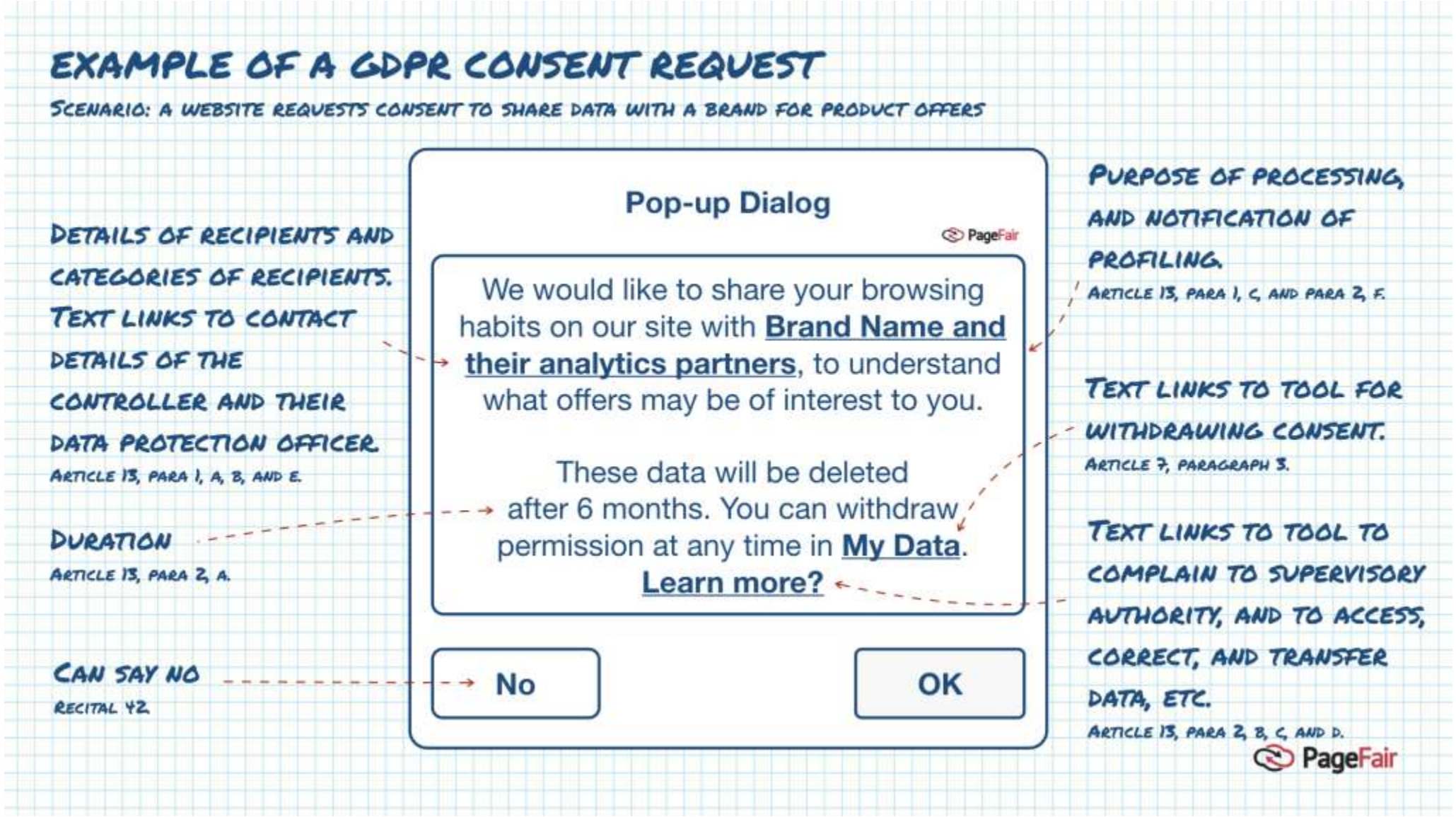
Mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, (ex : notification violation de données idéalement au plus tard 72h après l'identification, modification des données collectées, changement de prestataire,…).

Constituer et regrouper la documentation nécessaire pour prouver votre conformité au règlement

Actualiser régulièrement pour assurer une protection des données en continu.

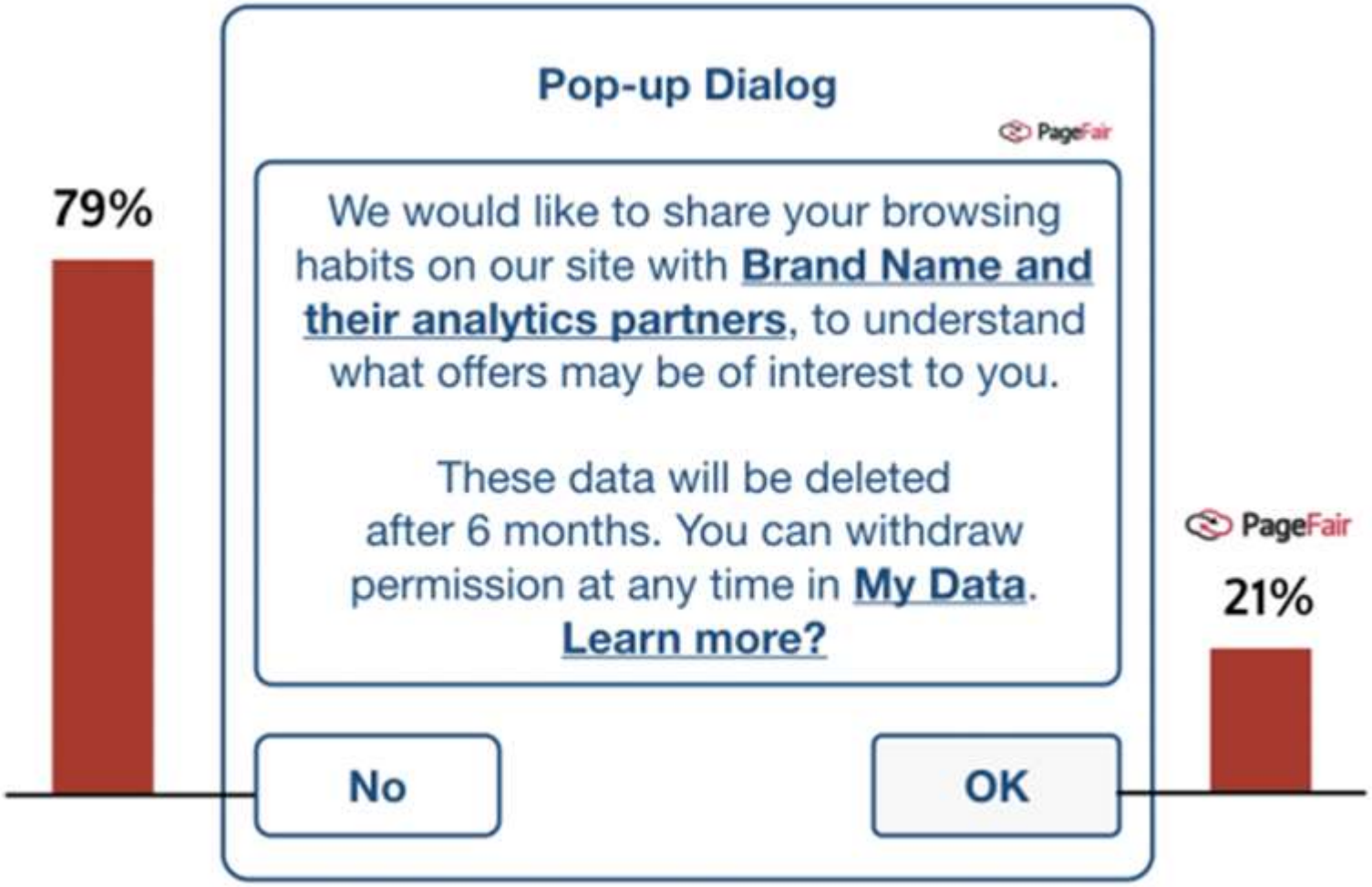
Source : https://www.cnil.fr/fr/comment-se-preparer-au-reglement-europeen-sur-la-protection-des-donnees

Mise en œuvre du consentement GDPR
=> exemple illustré



Mise en œuvre du consentement GDPR

=> étude menée par PageFair : à la question, face à un site web affichant cette popup de consentement GDPR, quel bouton choisiriez-vous ?



En conclusion

Au même titre que la **qualité**, la **performance**

=> la **sécurité** et la **protection des données à caractère personnel ne sont plus des options !**

Il faut voir le **GDPR** comme une **opportunité** pour remettre à plat les dérives dans la collecte, le traitement des données pour un **web responsable** et tenter **de regagner la confiance de tous !**

Selon le **Cabinet GARTNER** :
- avant 2020, environ 40% des organisations ne seront pas en conformité avec le GDPR;
- en 2023, ce pourcentage sera proche de zéro;

Source : https://www.gartner.com/doc/3635617/eu-privacy-impact-delivery-data

Et à suivre : le contenu du **nouveau règlement ePrivacy** portant sur **le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques**

Père Noël, nous savons que vous avez constitué un fichier avec les noms et coordonnées des personnes en les catégorisant méchantes ou sages !