RGPD

Pascal Lafourcade

LIMOS

UNIVERSITÉ Clermont Auvergne

Audaces, mai 2019

Plan

Avant le 25 mai 2018

Après le 25 mai 2018

Conclusion

Plan

Avant le 25 mai 2018

Après le 25 mai 2018

Conclusion

CNIL créé en 1978

Commission nationale de l'informatique et des libertés

BUT

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

ANSSI créée le 7 juillet 2009

STAD

Système de Traitement Automatisé de Données

"Tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité".

Aucune définition précise dans la loi

Dans les faits c'est presque tout :

3 acteurs

Utilisateur

Responsable

Pirate

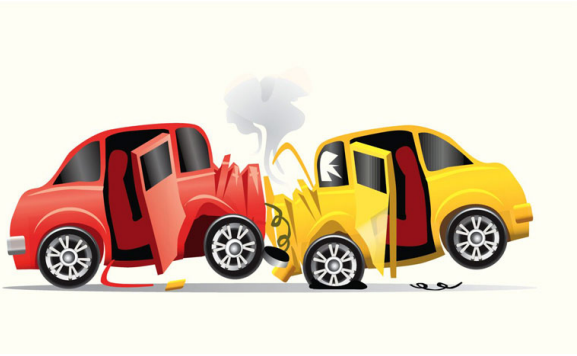
Plan

Avant le 25 mai 2018

Après le 25 mai 2018

Conclusion

RIP

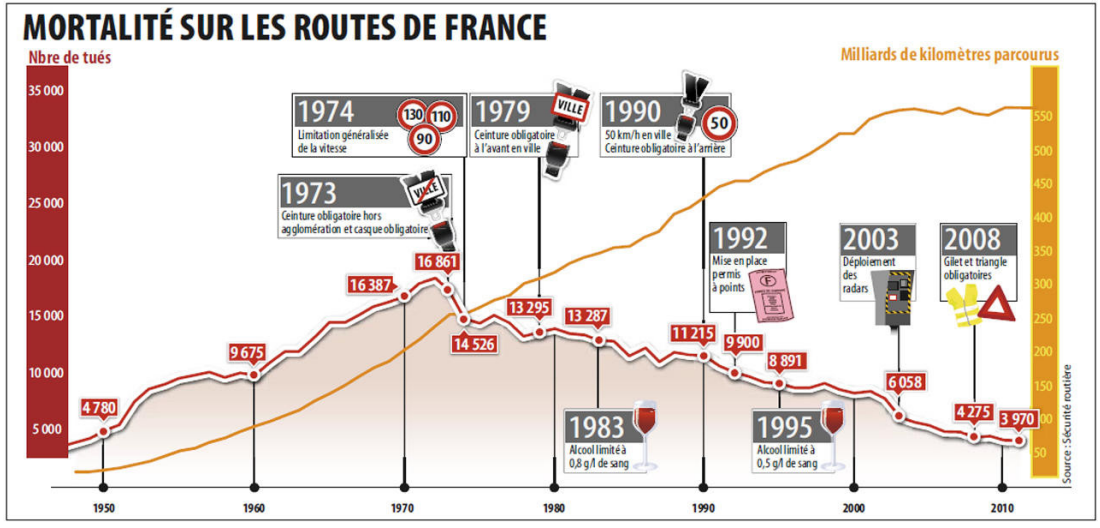


RIP

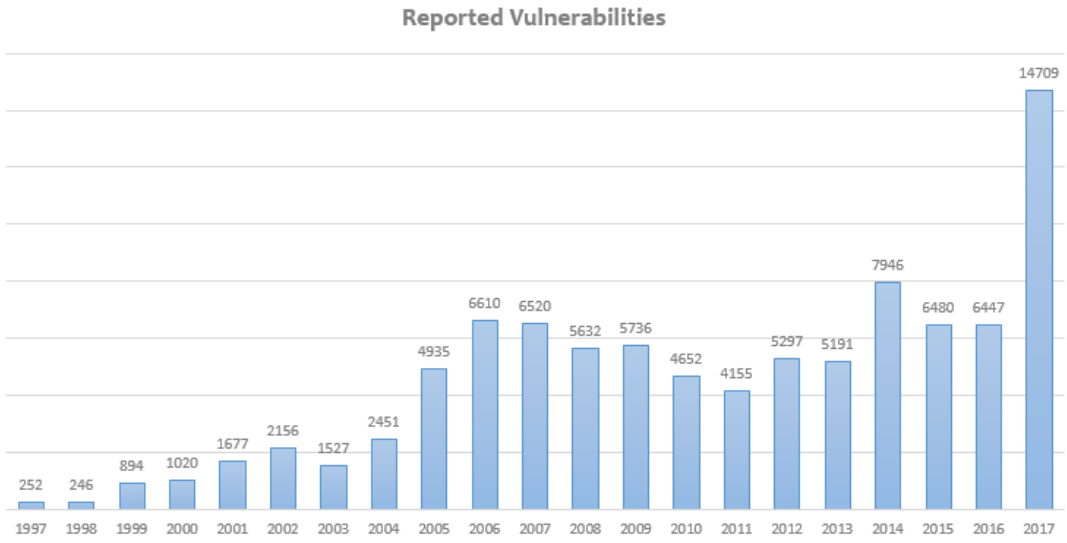
NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12

RIP

NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12

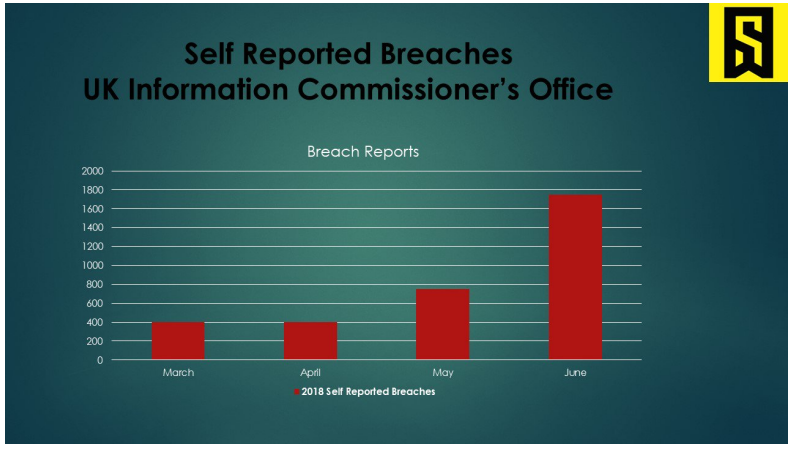

MORTALITÉ SUR LES ROUTES DE FRANCE
Nbre de tués
Milliards de kilomètres parcourus
35 000
30 000
25 000
20 000
15 000
10 000
5 000
550
500
450
400
350
300
250
200
150
100
50
1974
Limitation généralisée de la vitesse
130
110
90
1979
Ceinture obligatoire à l'avant en ville
VILLE
1990
50 km/h en ville
Ceinture obligatoire à l'arrière
50
1973
Ceinture obligatoire hors agglomération et casque obligatoire
VILLE
1992
Mise en place permis à points
2003
Déploiement des radars
2008
Gilet et triangle obligatoires
4 780
9 675
16 387
16 861
14 526
13 295
13 287
11 215
9 900
8 891
6 058
4 275
3 970
1983
Alcool limité à 0,8 g/l de sang
1995
Alcool limité à 0,5 g/l de sang
1950
1960
1970
1980
1990
2000
2010
Source : Sécurité routière

L'argus



Règlement Général sur la Protection des Données

GDPR : General Data Protection Regulation



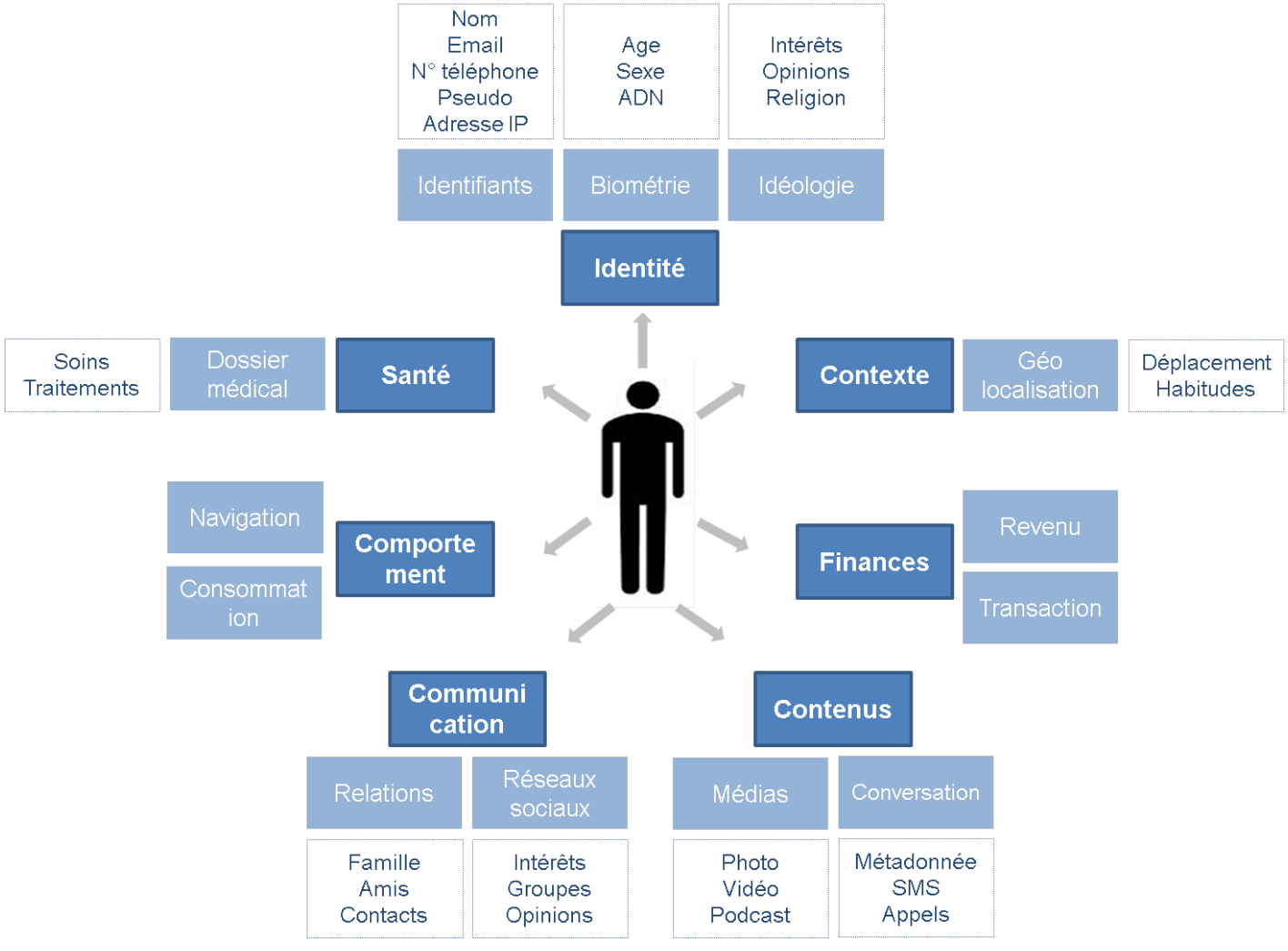
Qui est touché ?

TOUT LE MONDE !

5 types de données

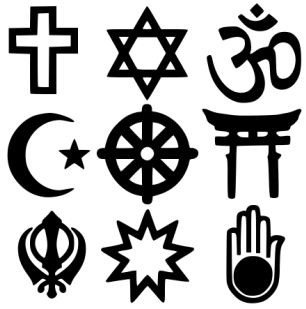
1. neutres
2. personnelles
3. sensibles
4. pseudonymisées
5. anonymisées

Qu'est-ce qu'une donnée personnelle ?



Toutes informations relatives à une personne physique qui peuvent être utilisées pour re-indentifier la personne.

Qu'est-ce qu'une donnée personnelle **sensible**?



Collecte sans consentement préalable écrit, clair et explicite

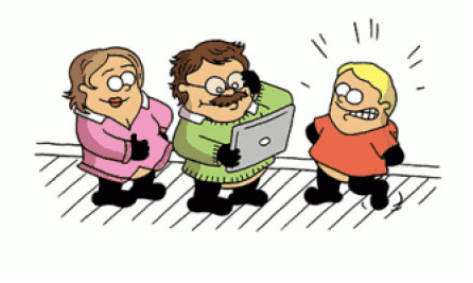
Plus de droits pour vos données !

Sanction

Plus de transparence

Droit à l'oubli

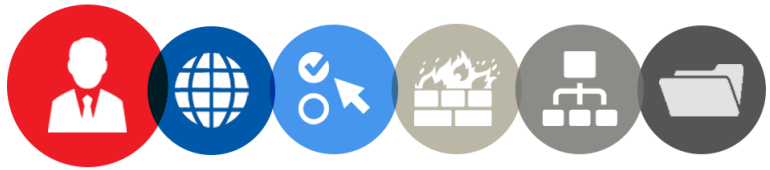
Guichet unique



Protection des mineurs

Portabilité

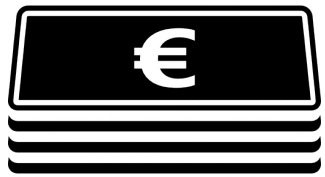
RPGD : en 6 étapes @CNIL



1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

Sanctions

20 millions



ou 4 %

Les principes fondamentaux

- le traitement loyal et licite;
- la limitation des finalités;
- la minimisation et la conservation des données.

Transparence

- Procédure consultation, rectification et suppression
- Informer les utilisateurs 72h après un attaque
- La protection des données dès la conception et par défaut
- Avoir des sytème à jour par rapport à l'état de l'art MD5 SHA-1

Les collectivités doivent

- tenir un registre de leurs activités de traitement,
- notifier à la CNIL, voire aux personnes concernées, les violations de données personnelles,
- effectuer des analyses d'impact sur la vie privée et les libertés pour certains traitements à risques
- encadrer les opérations sous-traitées dans les contrats de prestation de services,
- veiller à garantir la confidentialité des données,
- organiser la prise en charge des demandes d'exercice des droits,
- organiser la détection et la gestion des incidents de sécurité.

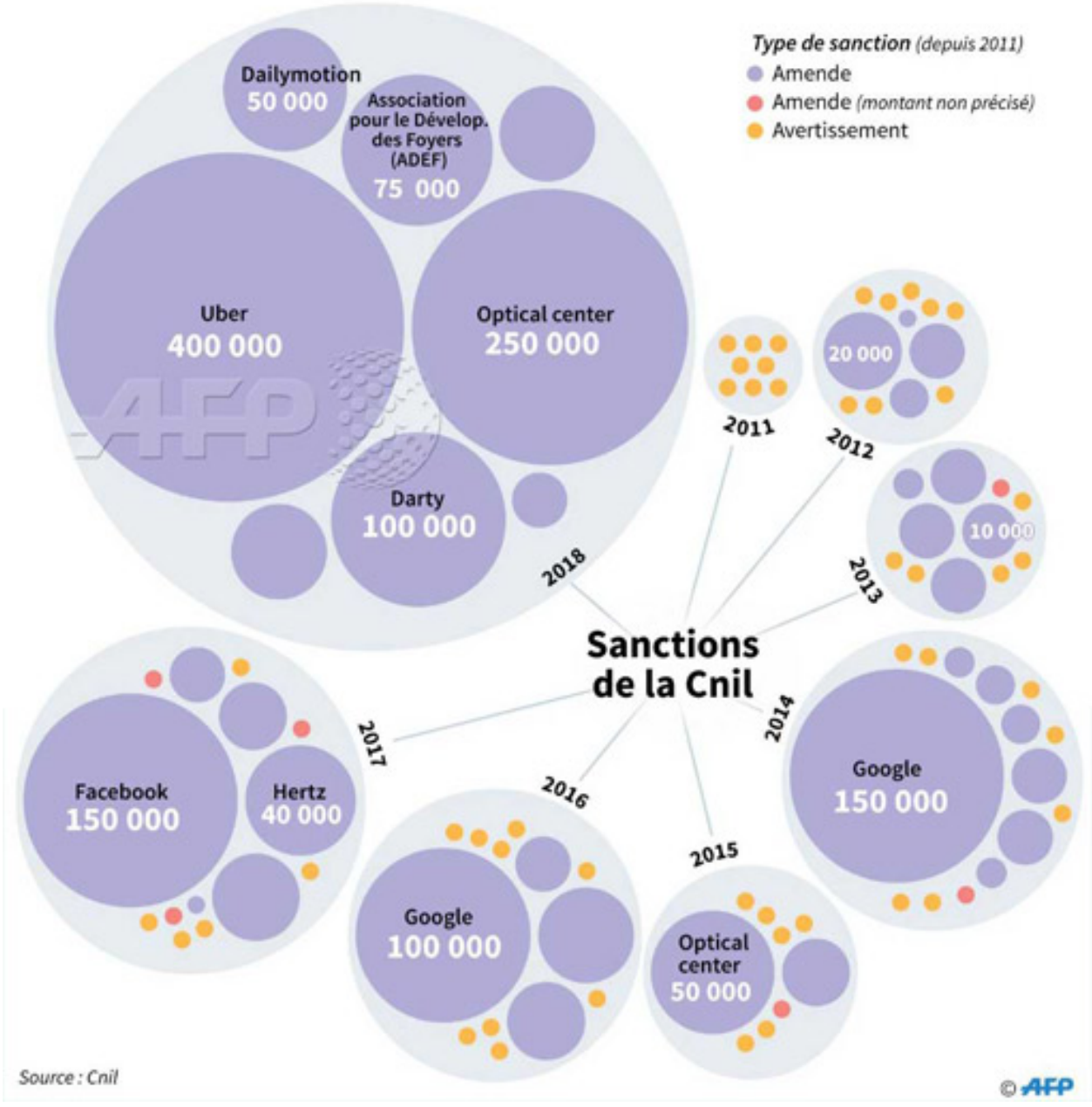
Bilan après 6 mois en France

- 32 000 organismes ont 1 DPO: 15000 DPO contre 5000 CIL
- 100 notifications de violations, environ 7 par jour
- 7 millions de visites sur le site de la CNIL
- 130 000 téléchargements du PIA de la CNIL
- 9 700 plaintes
- plus de 345 plaintes transfrontalières
- Conception d'un MOOC
- 59,000 fuites de donnée en EU

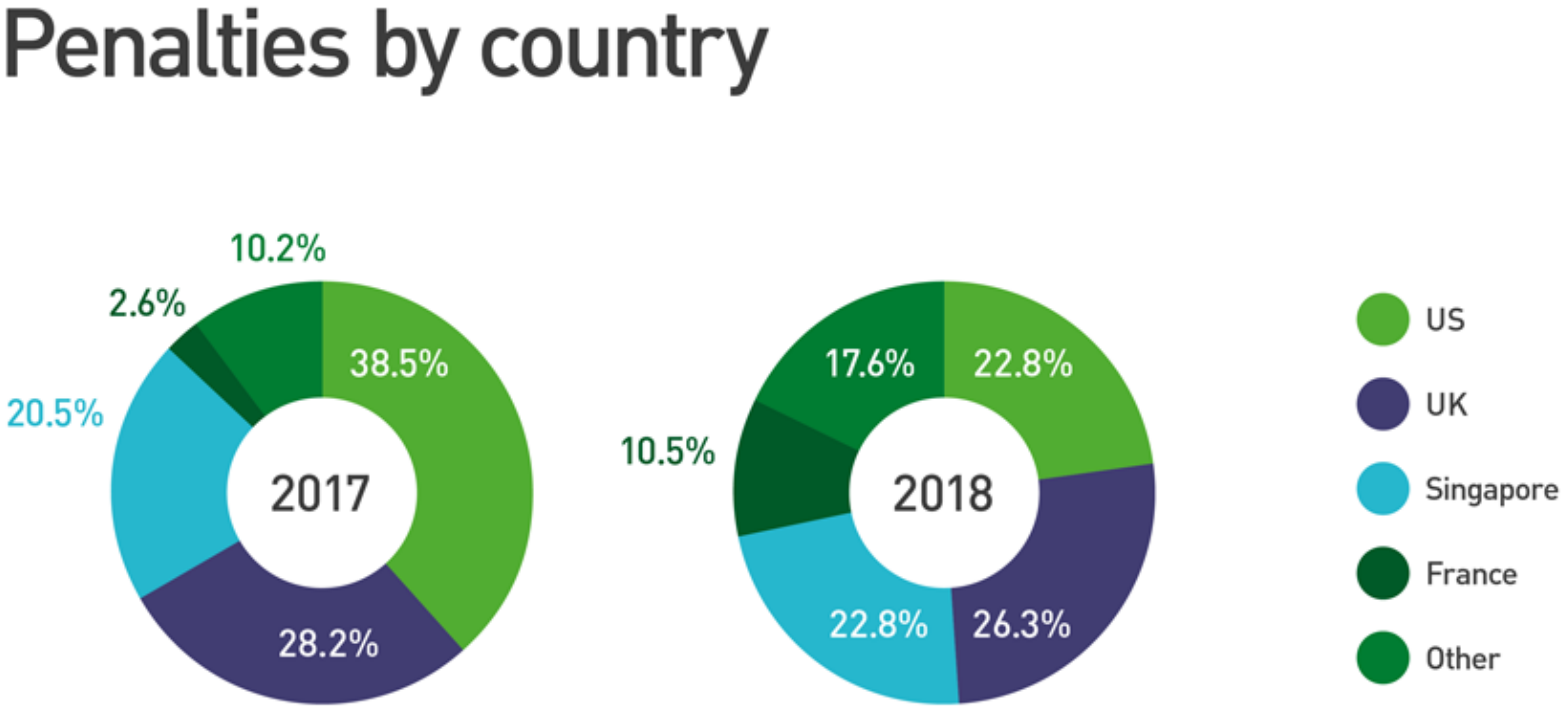
Bilan après 6 mois en France

24 Juillet 2018 : Sanction de 50 000 € de la CNIL à l'encontre de la société DAILYMOTION, mot de passe stocké en clair temporairement.
15 Aout 2018 : Sanction de 30 000 € par la CNIL à l'encontre de l'Office Public de l'Habitat de Rennes Métropole
21 janvier 2019 50 Millions € à Google : le manque de transparence, le manque d'information adéquate, l'absence de consentement explicite préalablement recueilli.

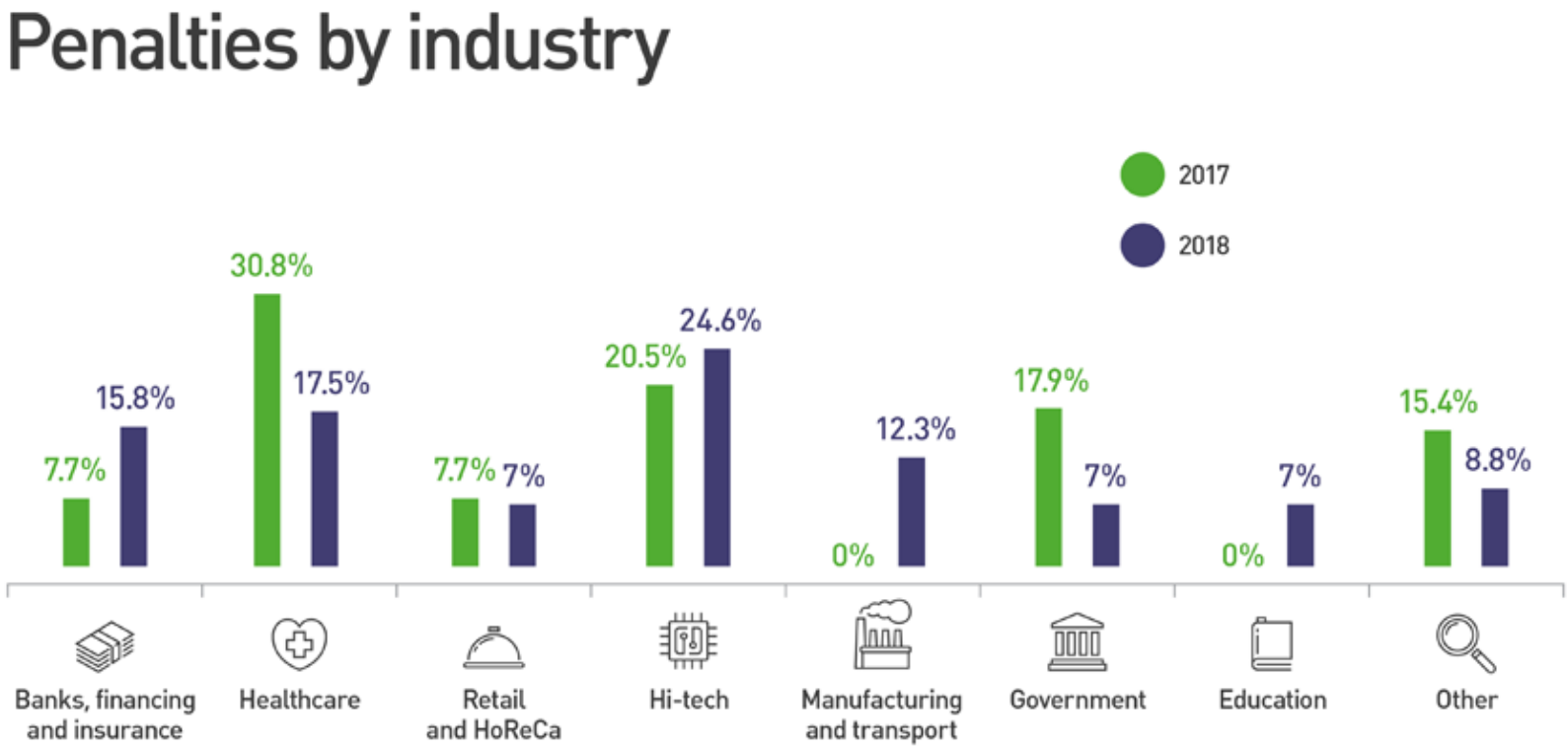
Sanctions de la CNIL



Par pays

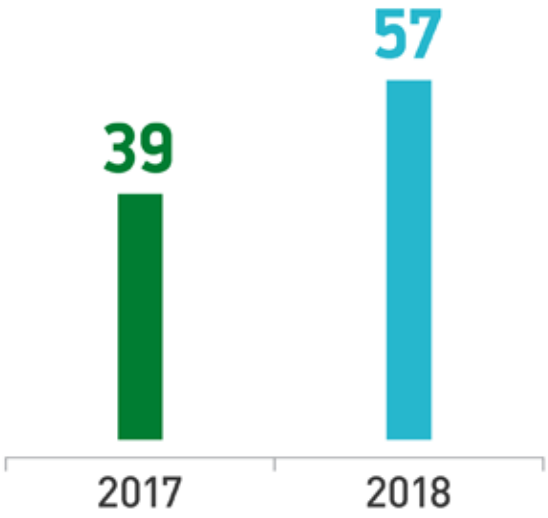

Penalties by country
10.2%
2.6%
38.5%
20.5%
2017
28.2%
17.6%
22.8%
10.5%
2018
22.8%
26.3%
US
UK
Singapore
France
Other

Par industries

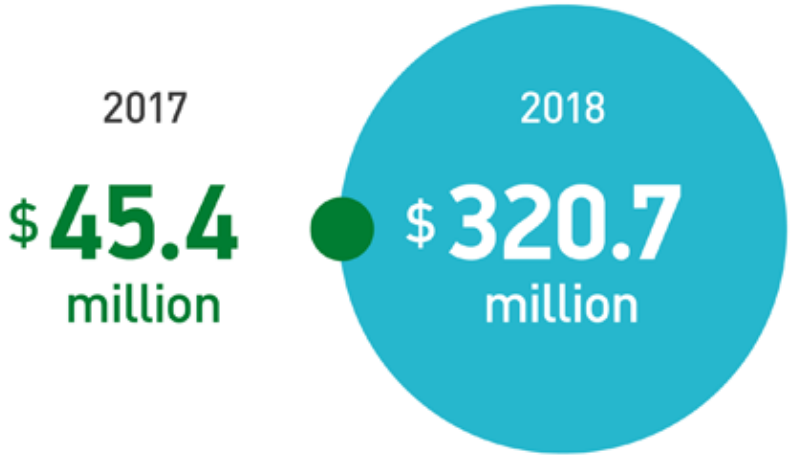


Évolution

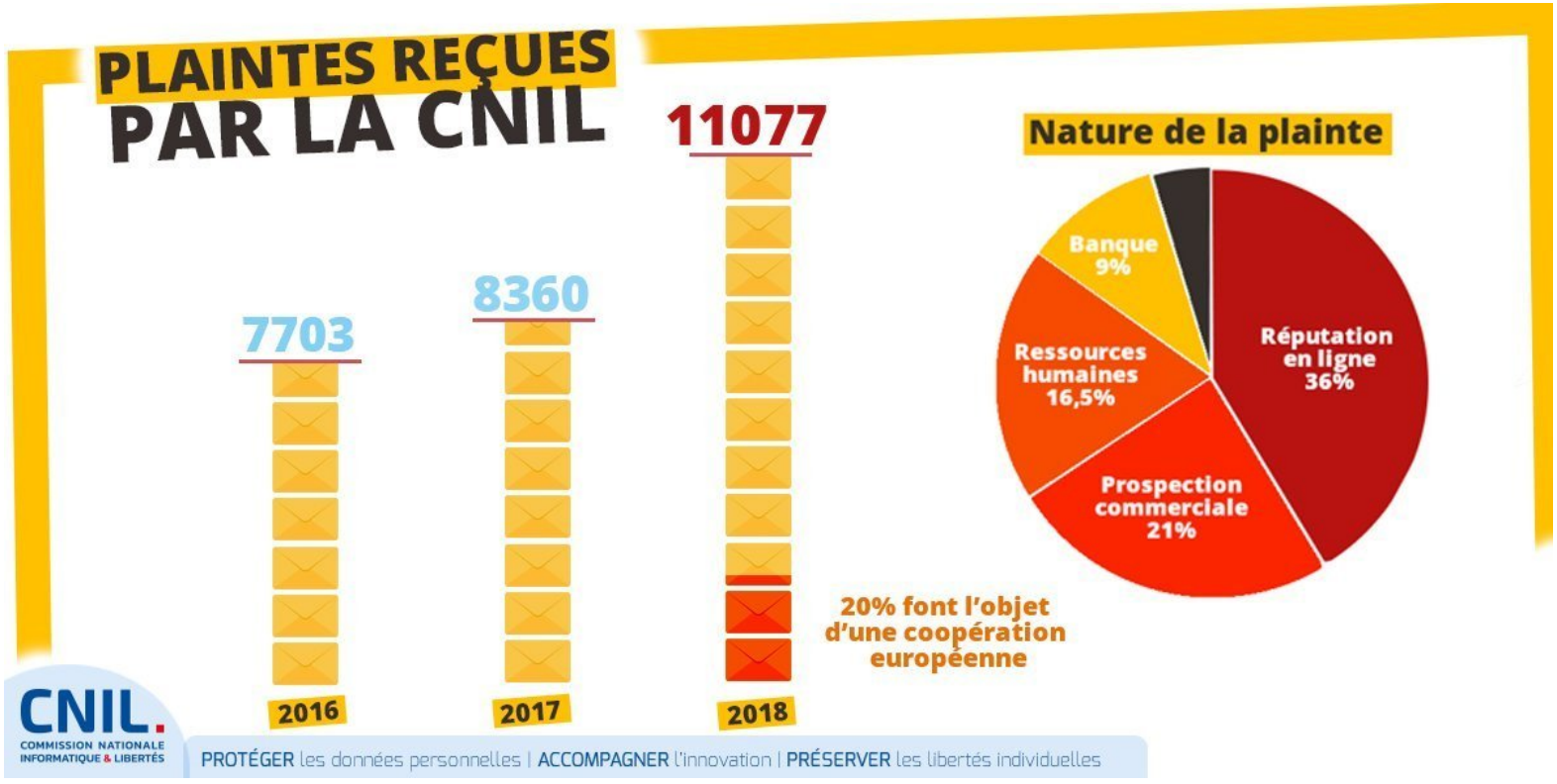
Number of data breach penalties



Total amount of penalties, million of US dollars

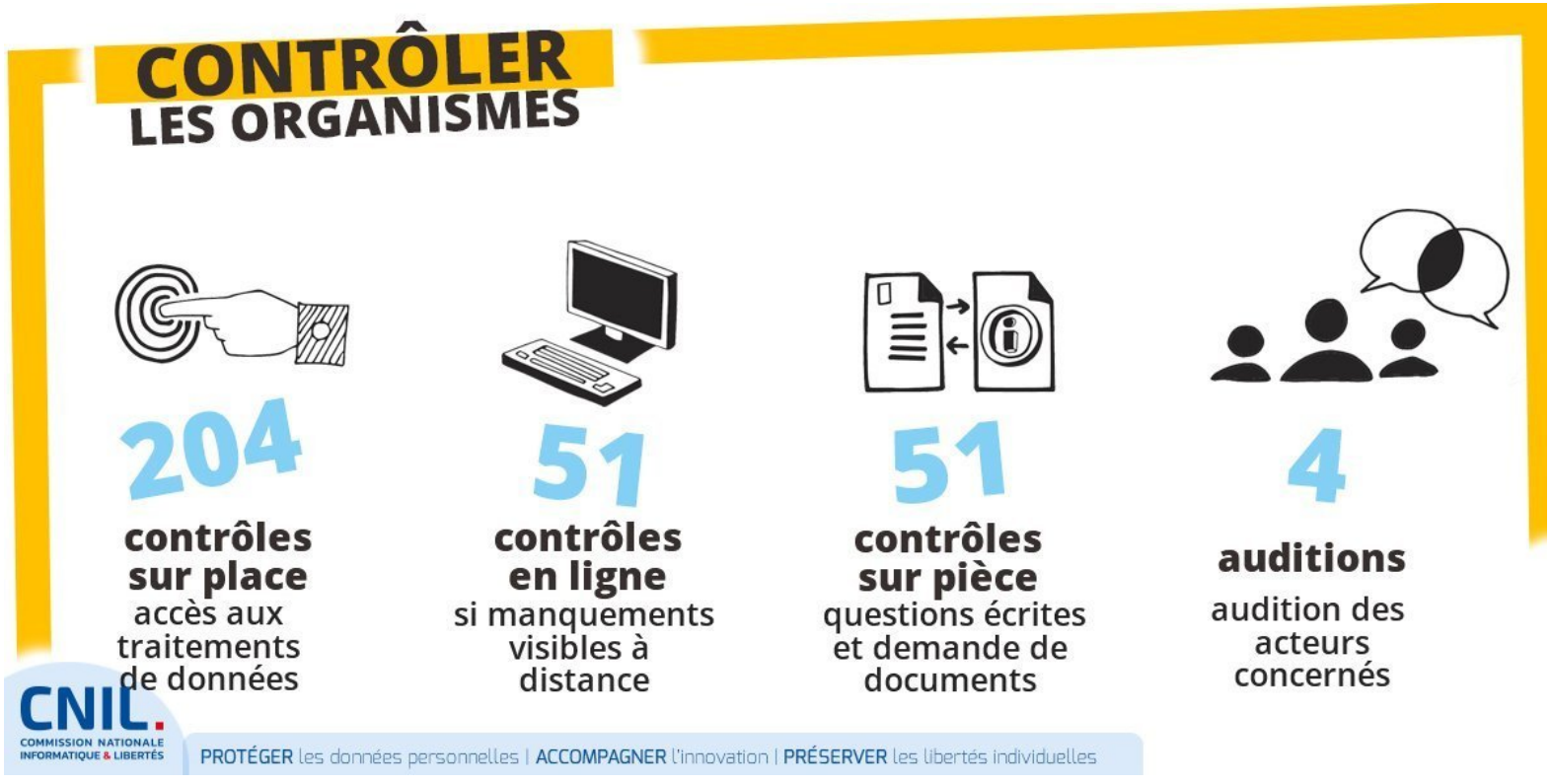


Plaintes déposées 2018

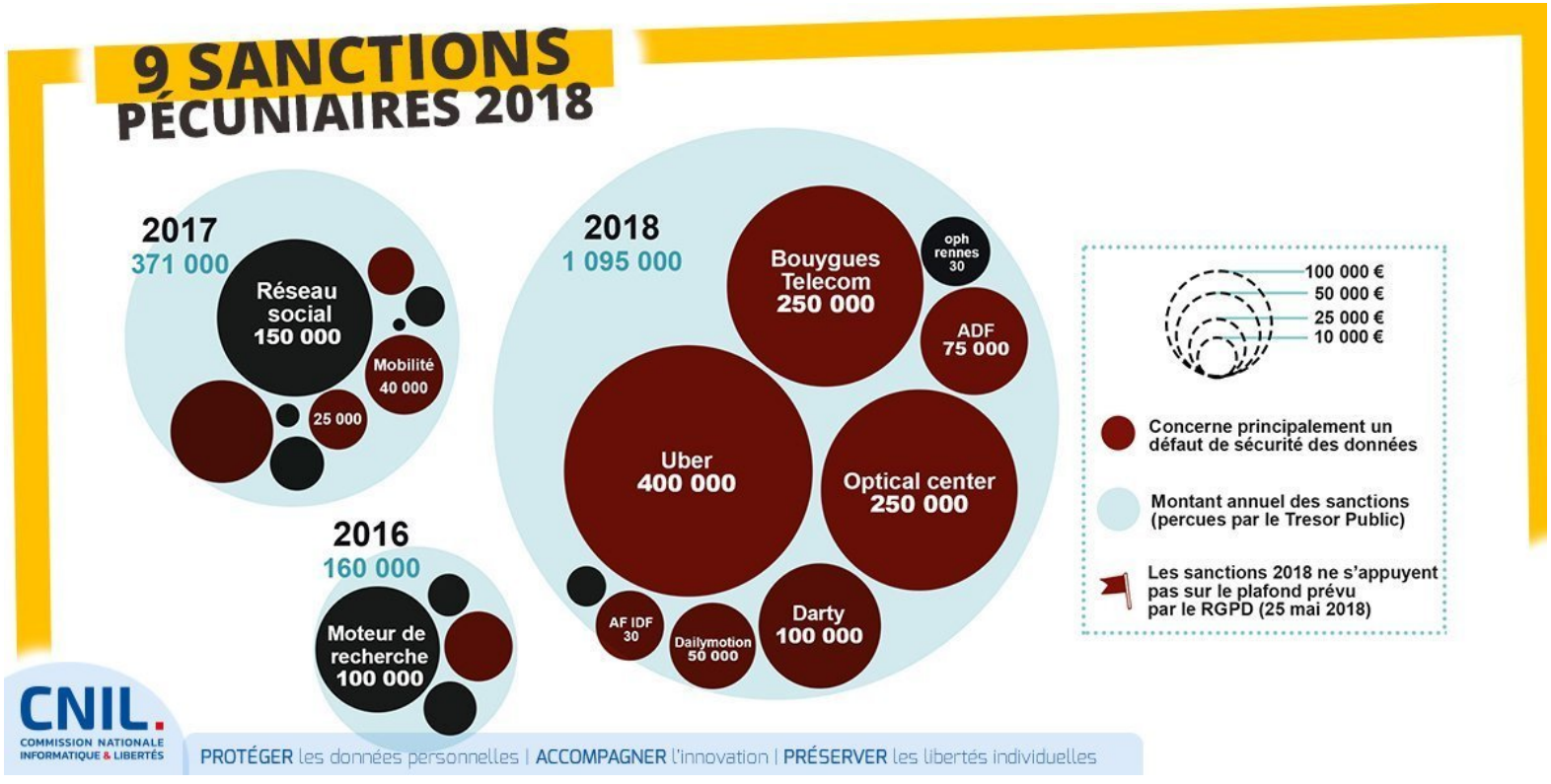


Tendances 2018

Contrôles 2018



Sanctions 2018

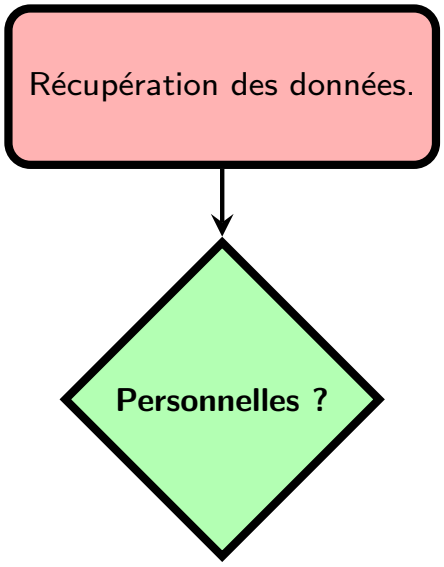


1 an après

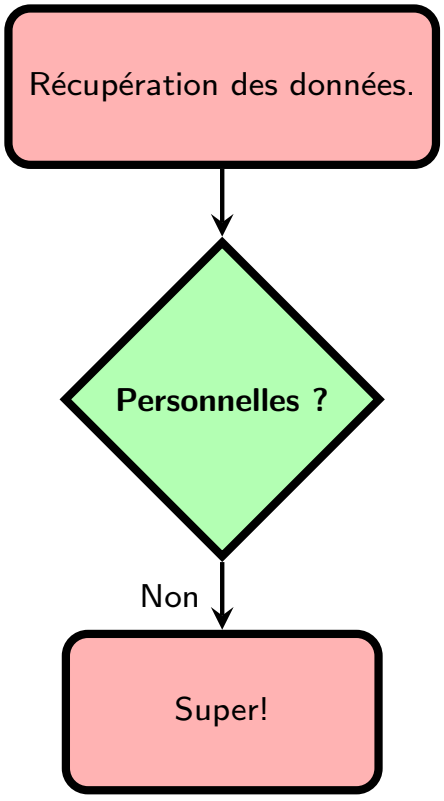
"70 % des Français se disent aujourd'hui plus sensibles aux problématiques de protection des données."

- 2 044 notifications de violation de données en France
- 89 271 au niveau européen ;
- Plus de 19 000 DPO désignés par plus de 53 000 organismes
- Plus de 8,1 millions de visites depuis un an cnil.fr

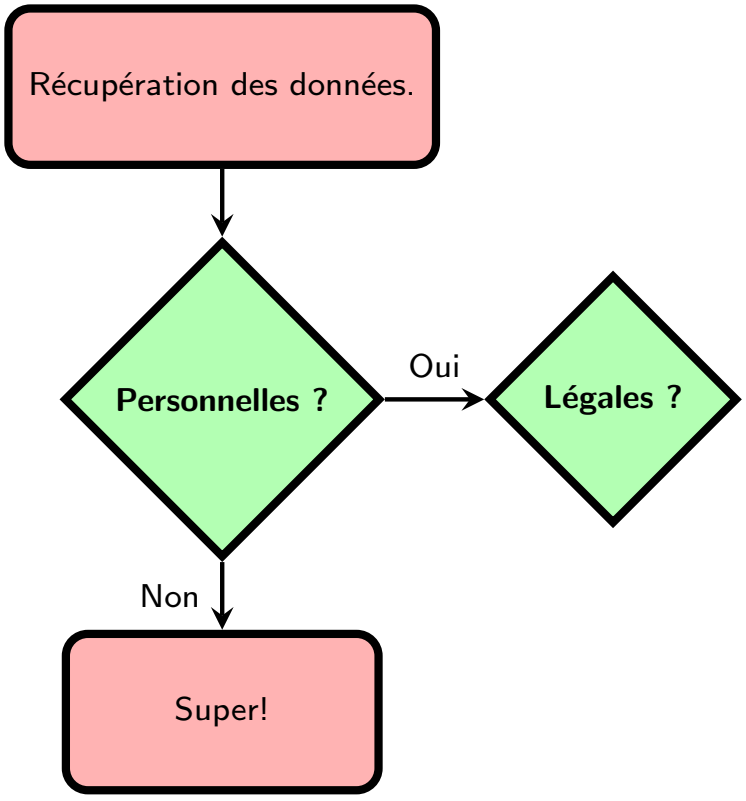
Cas d'étude 1



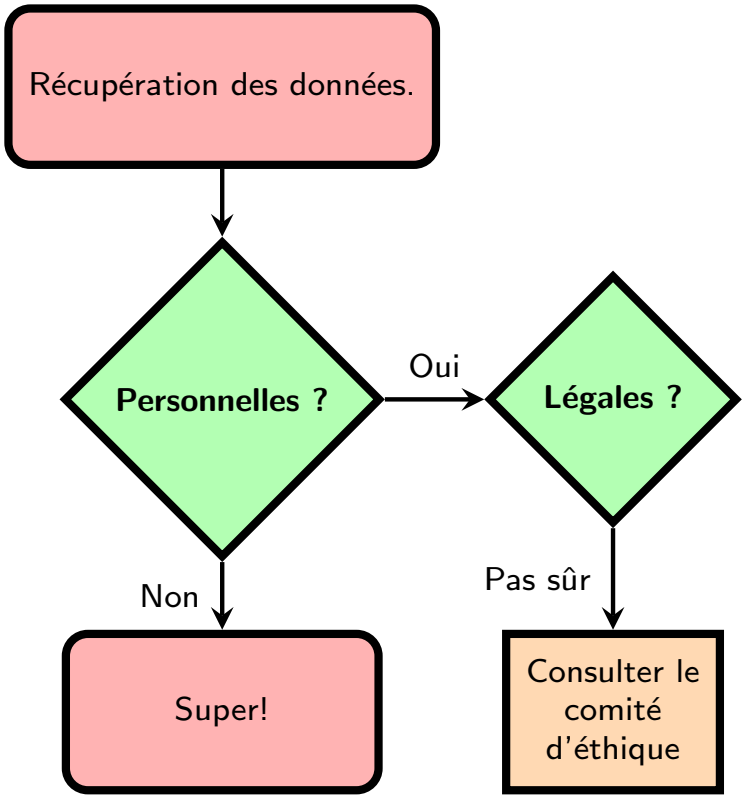
Cas d'étude 1



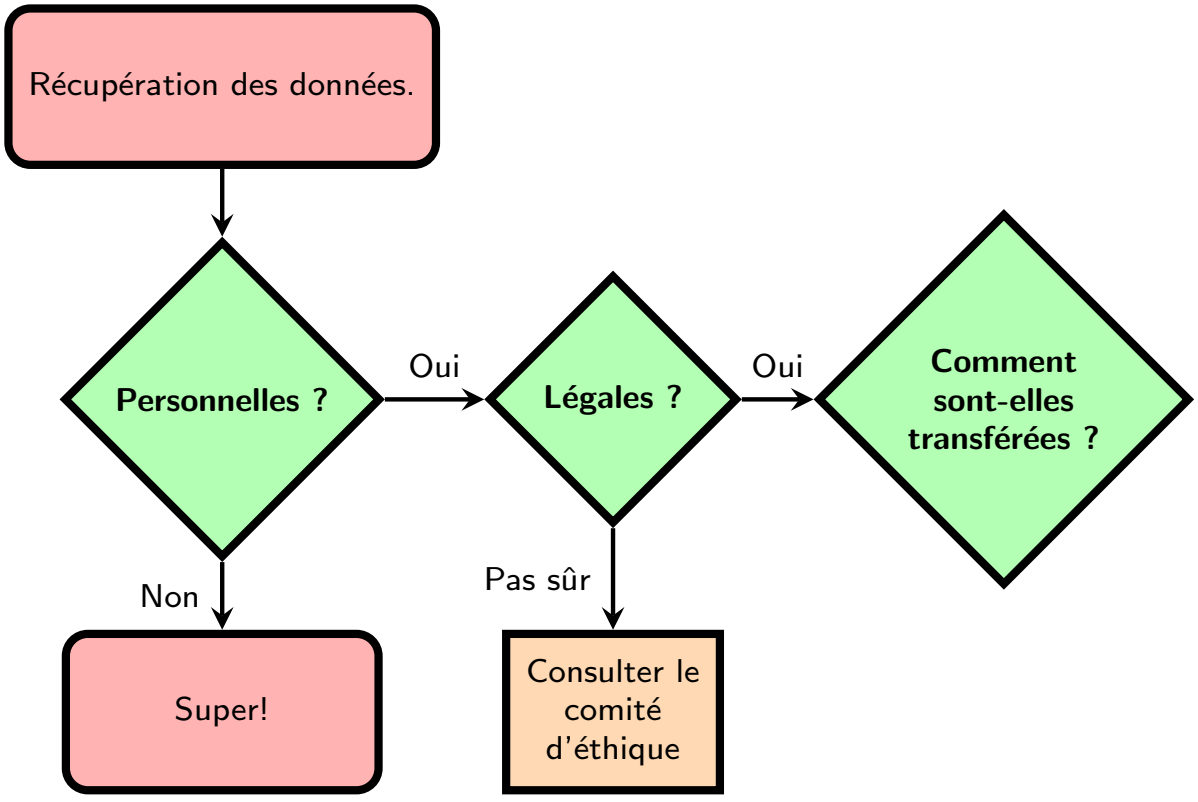
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Non
Super!

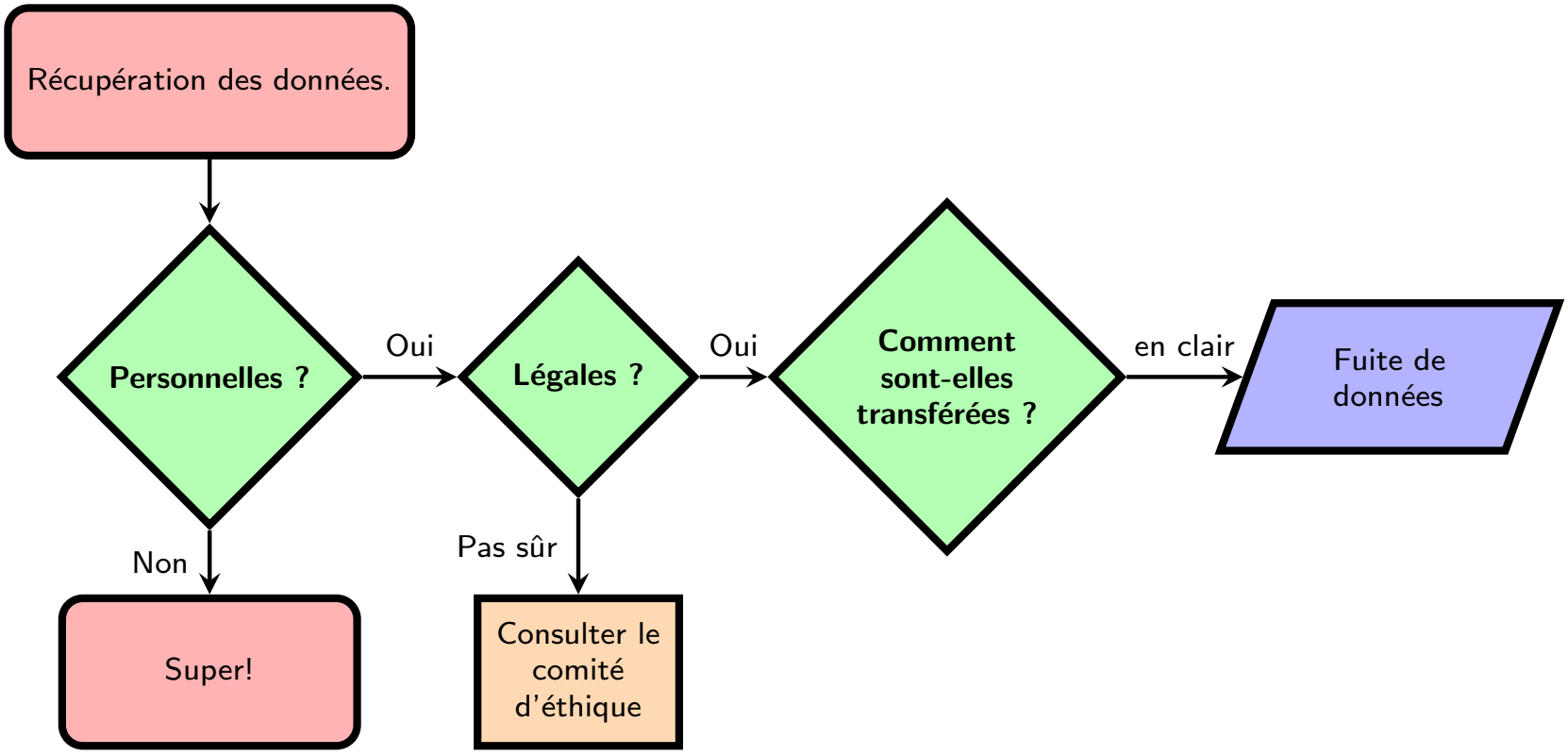
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Non
Pas sûr
Super!
Consulter le comité d'éthique

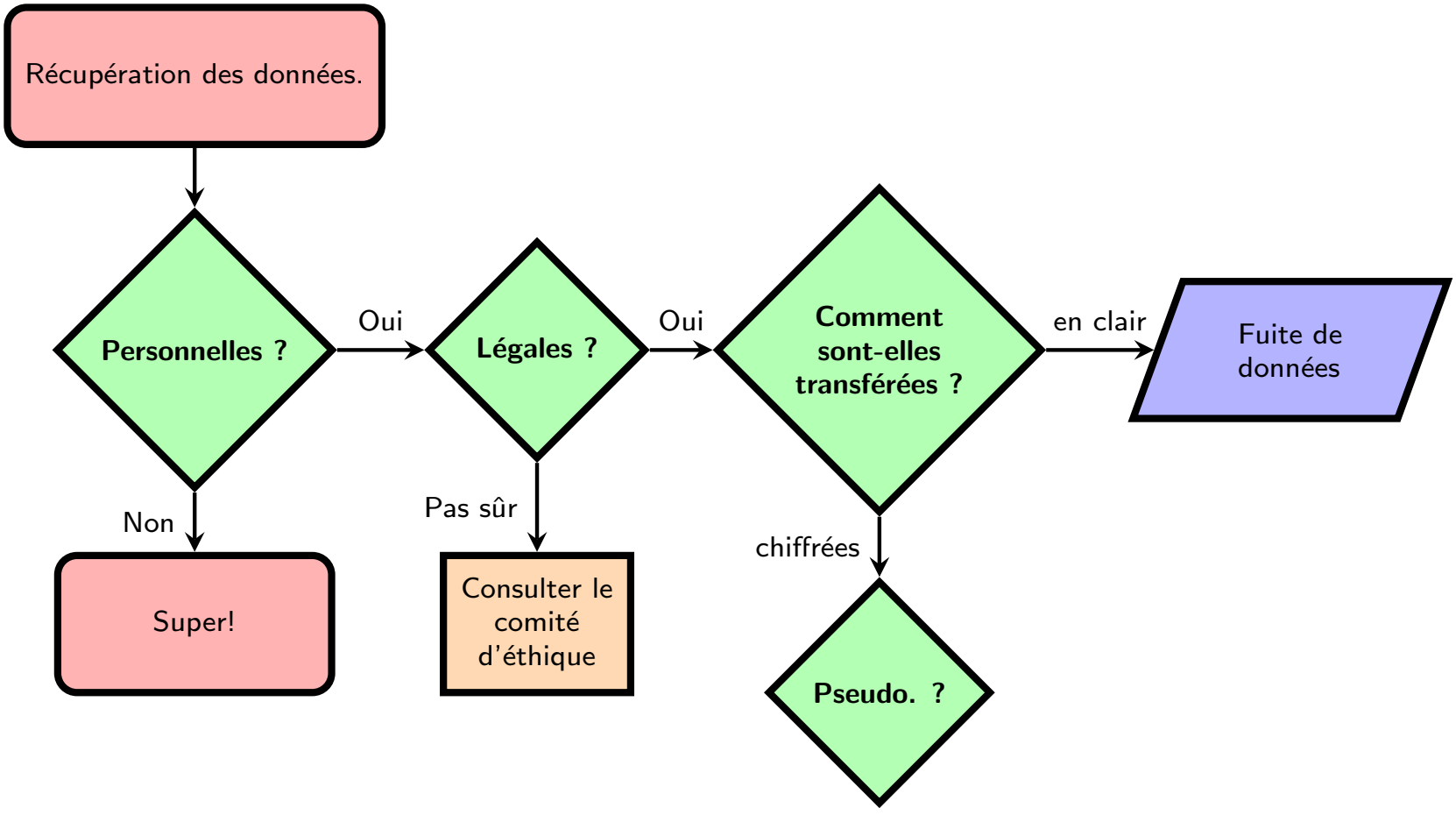
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Oui
Comment sont-elles transférées ?
Non
Super!
Pas sûr
Consulter le comité d'éthique

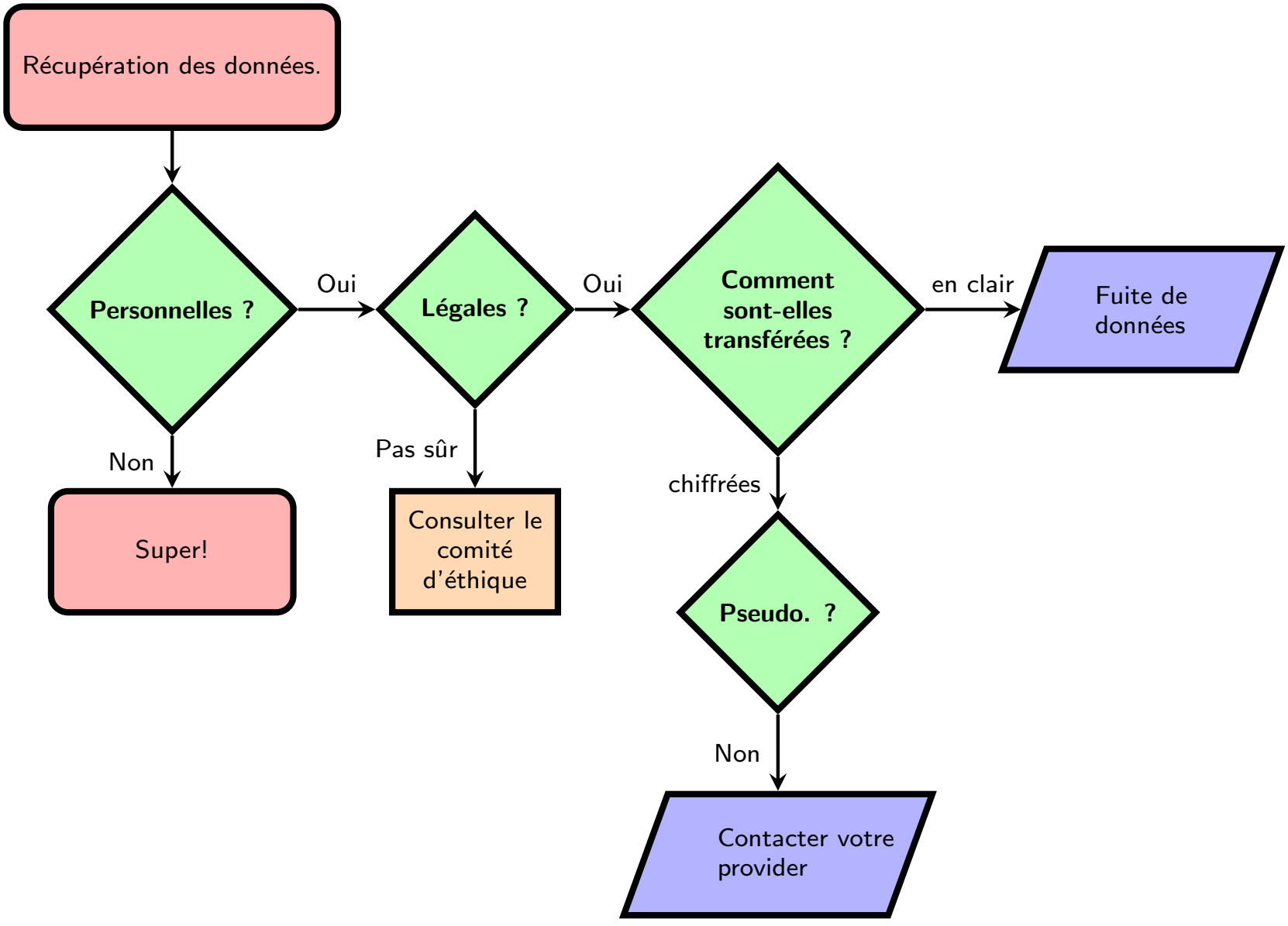
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Oui
Comment sont-elles transférées ?
en clair
Fuite de données
Non
Super!
Pas sûr
Consulter le comité d'éthique

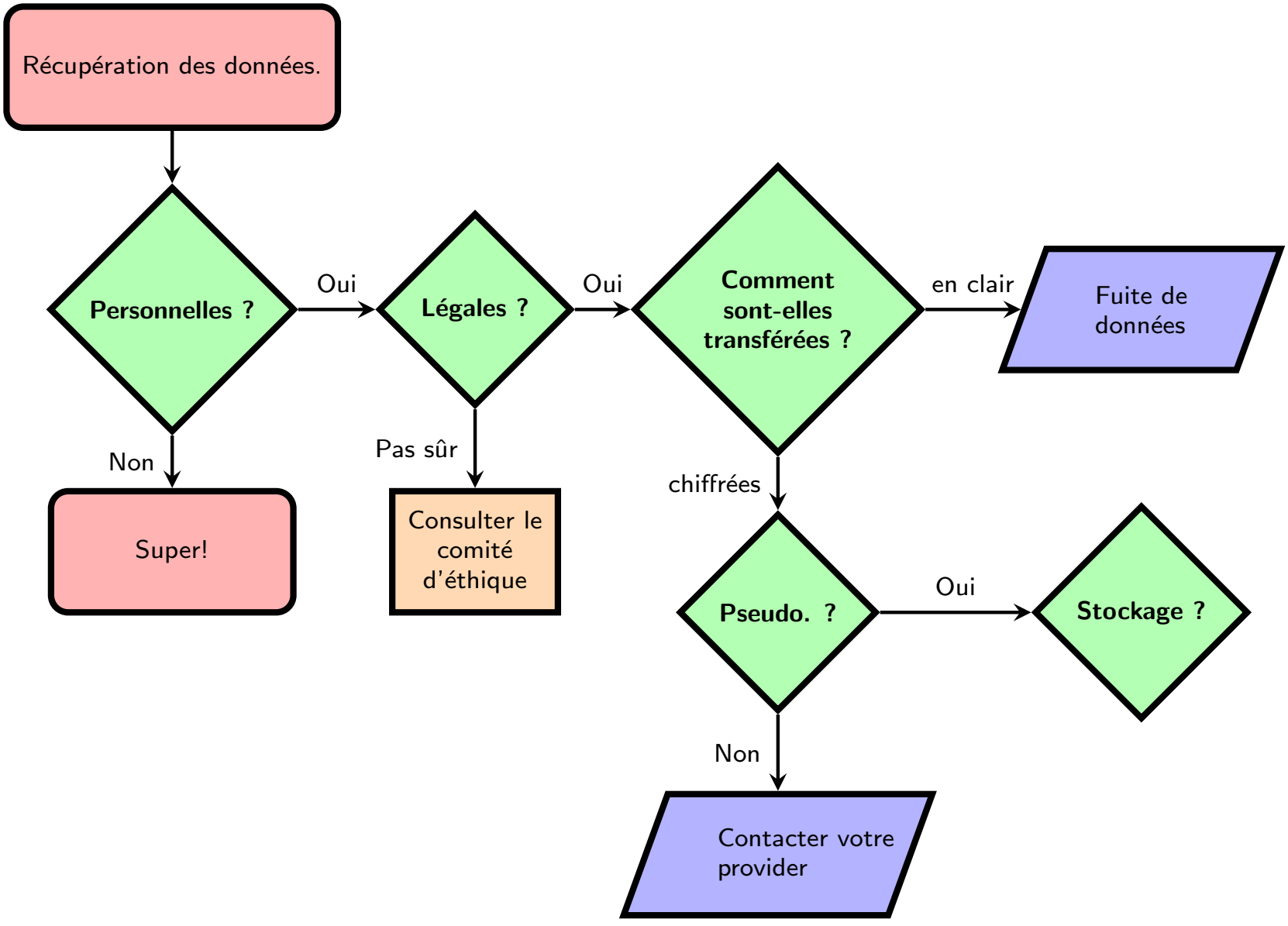
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Oui
Comment sont-elles transférées ?
en clair
Fuite de données
Non
Super!
Pas sûr
Consulter le comité d'éthique
chiffrées
Pseudo. ?

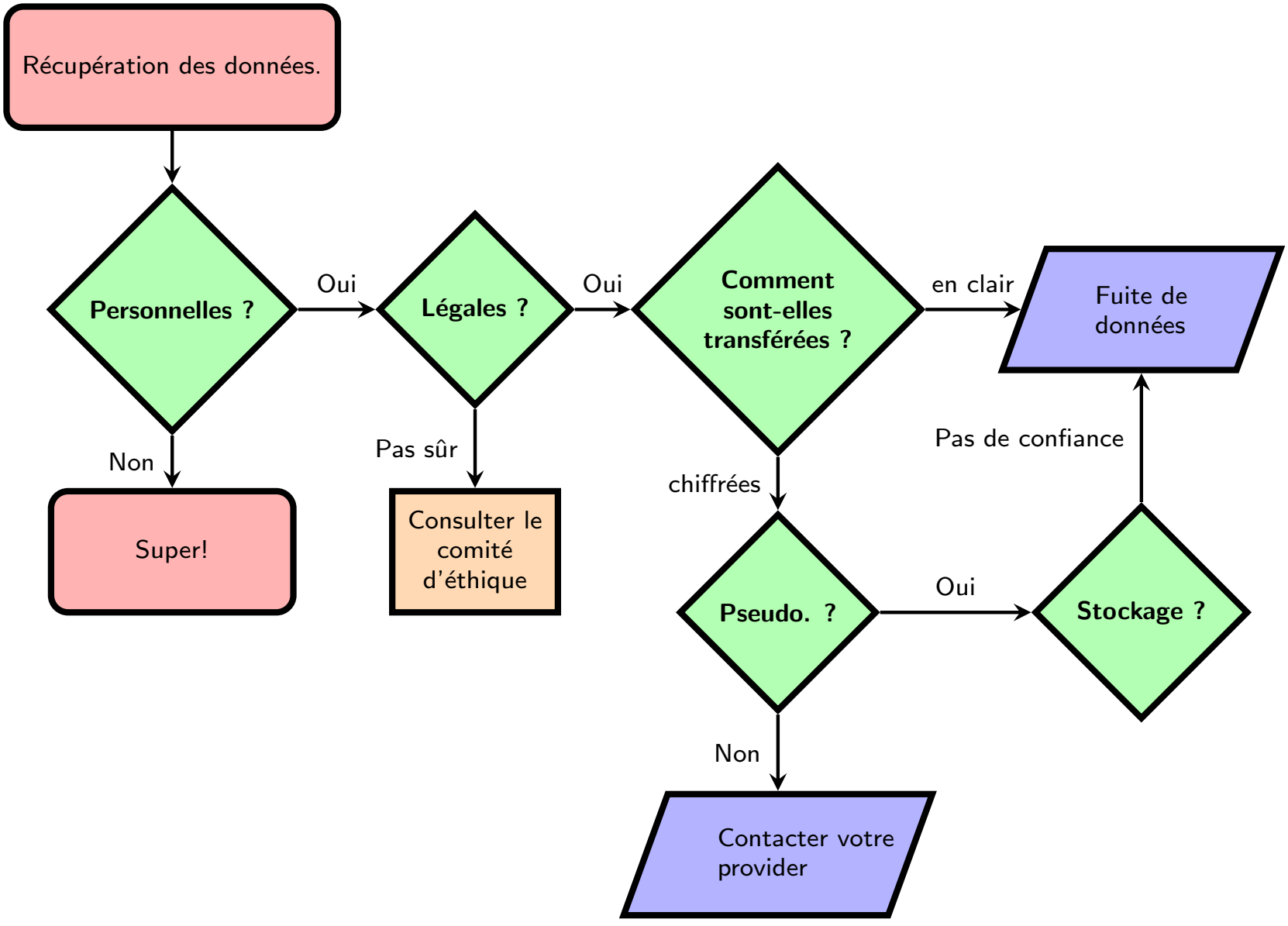
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Oui
Comment sont-elles transférées ?
en clair
Fuite de données
Non
Super!
Pas sûr
Consulter le comité d'éthique
chiffrées
Pseudo. ?
Non
Contacter votre provider

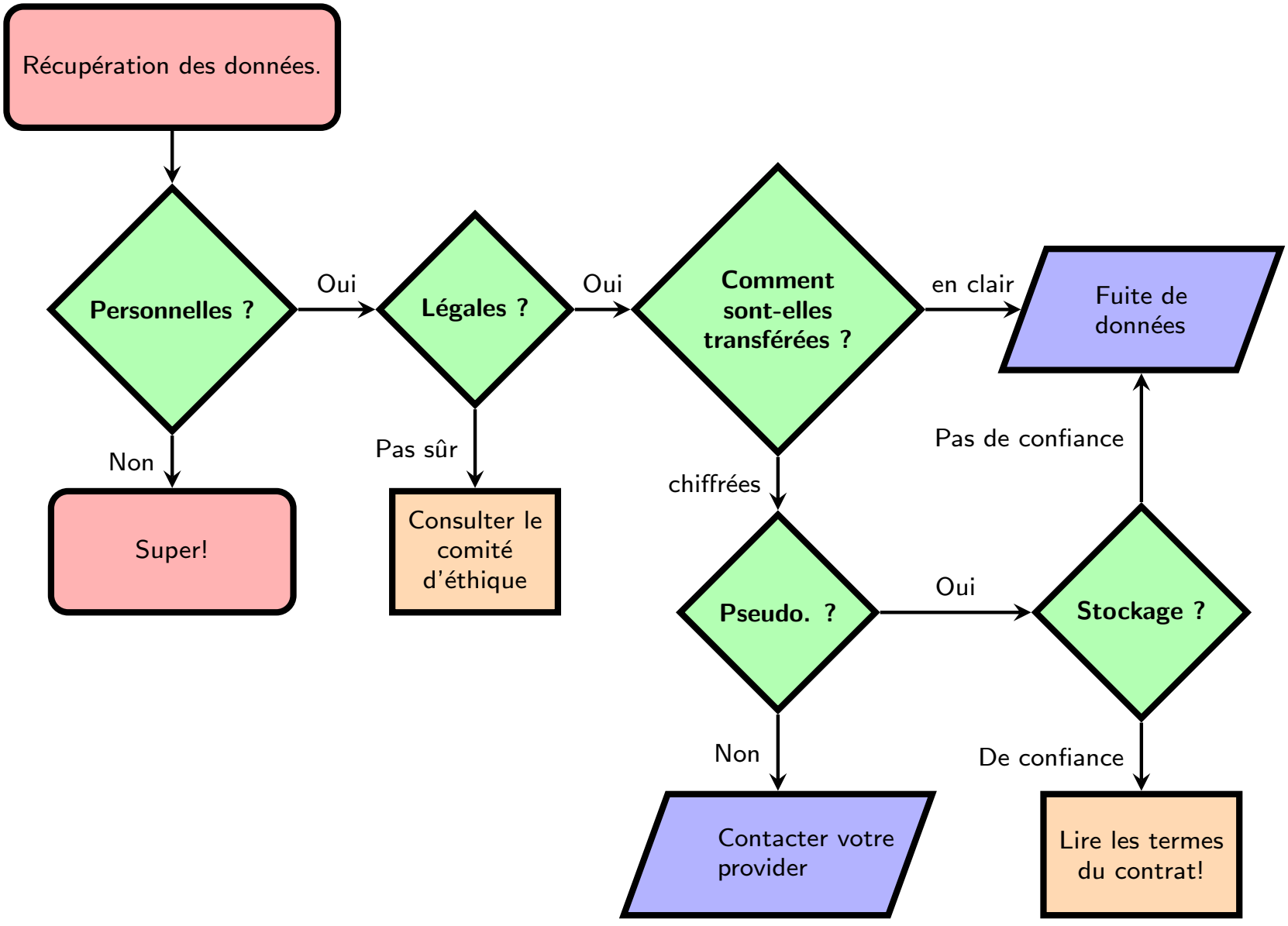
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Oui
Comment sont-elles transférées ?
en clair
Fuite de données
Non
Super!
Pas sûr
Consulter le comité d'éthique
chiffrées
Pseudo. ?
Oui
Stockage ?
Non
Contacter votre provider

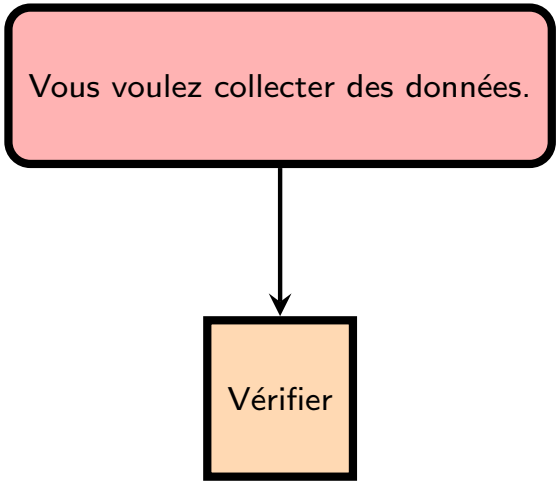
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Oui
Comment sont-elles transférées ?
en clair
Fuite de données
Non
Super!
Pas sûr
Consulter le comité d'éthique
chiffrées
Pas de confiance
Pseudo. ?
Oui
Stockage ?
Non
Contacter votre provider

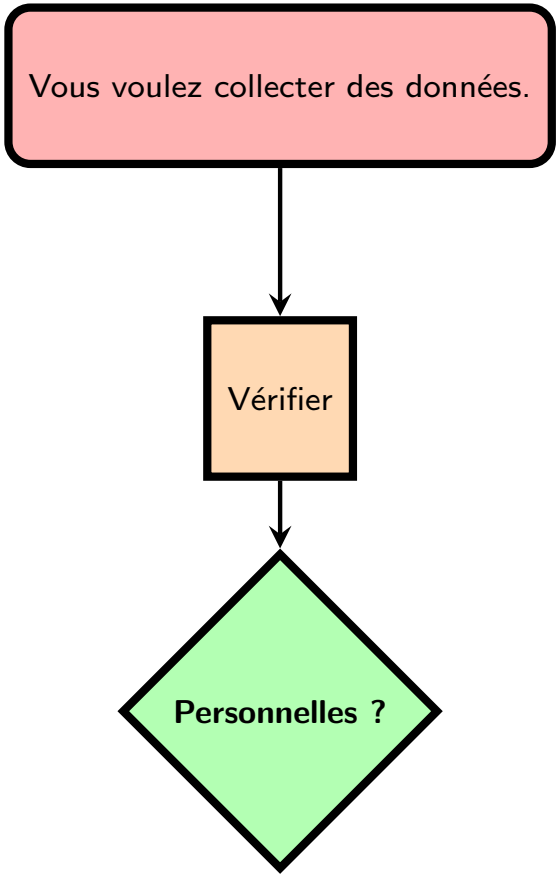
Cas d'étude 1


Récupération des données.
Personnelles ?
Oui
Légales ?
Oui
Comment sont-elles transférées ?
en clair
Fuite de données
Non
Super!
Pas sûr
Consulter le comité d'éthique
chiffrées
Pas de confiance
Pseudo. ?
Oui
Stockage ?
Non
Contacter votre provider
De confiance
Lire les termes du contrat!

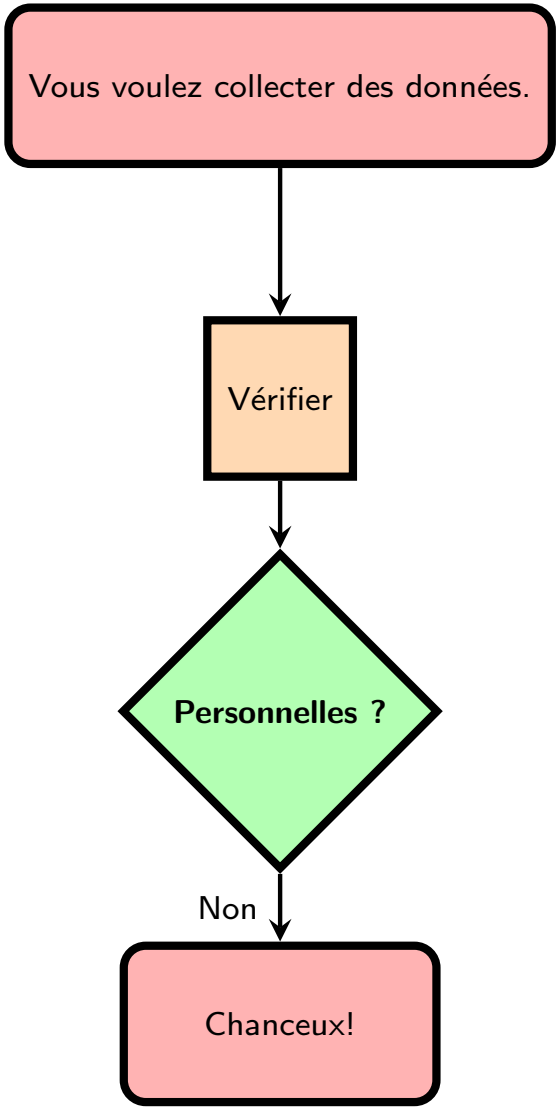
Cas d'étude 2 : Collecte de données



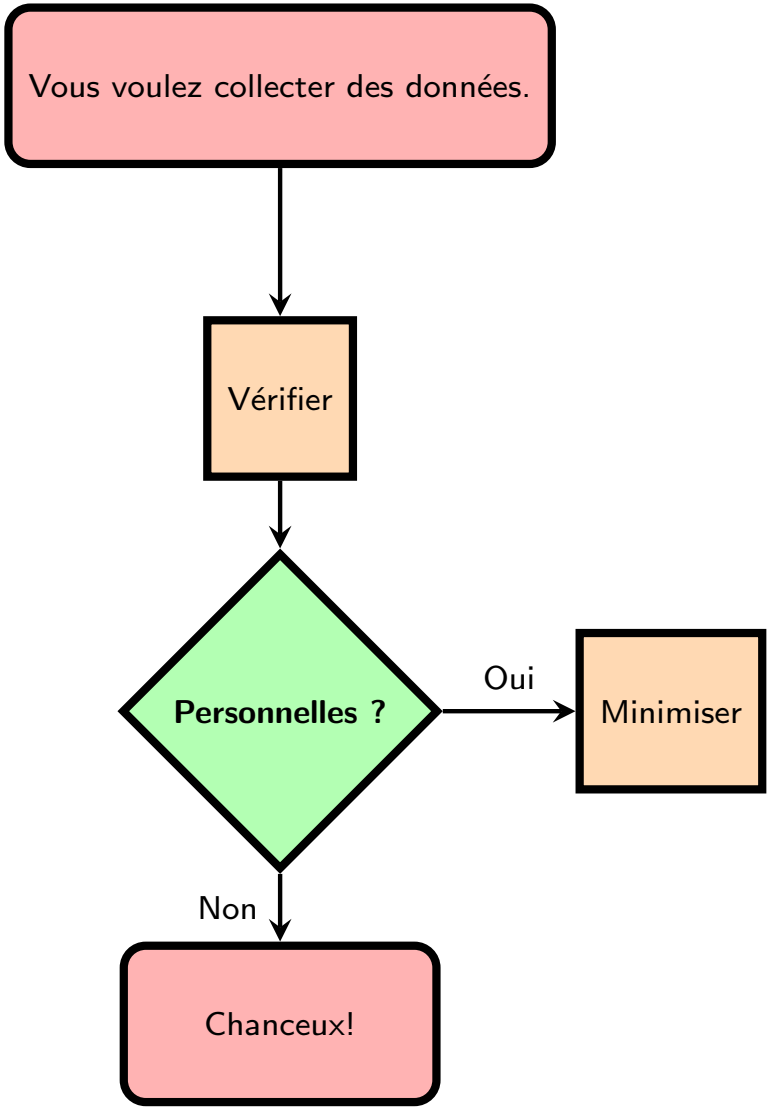
Cas d'étude 2 : Collecte de données



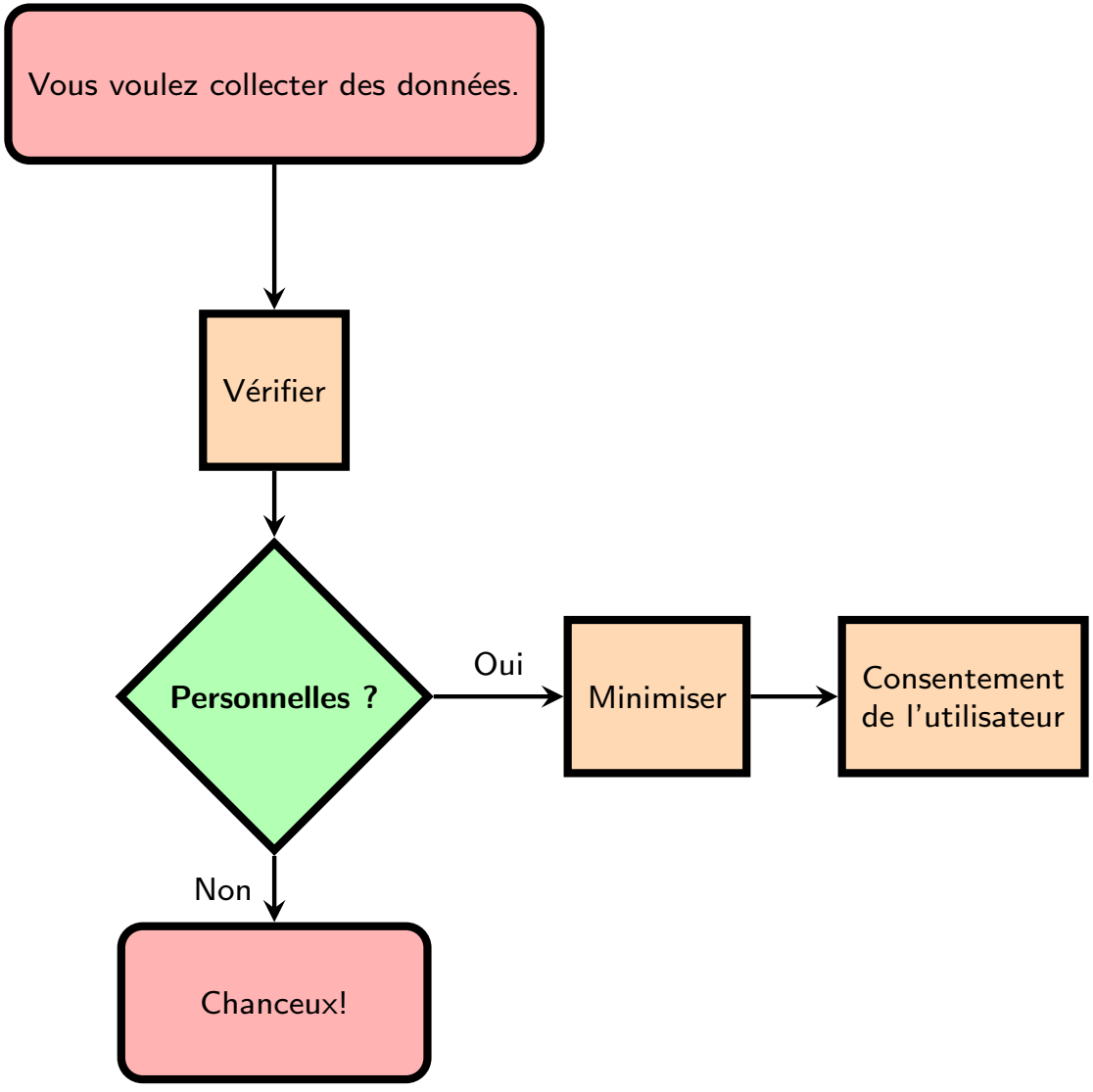
Cas d'étude 2 : Collecte de données



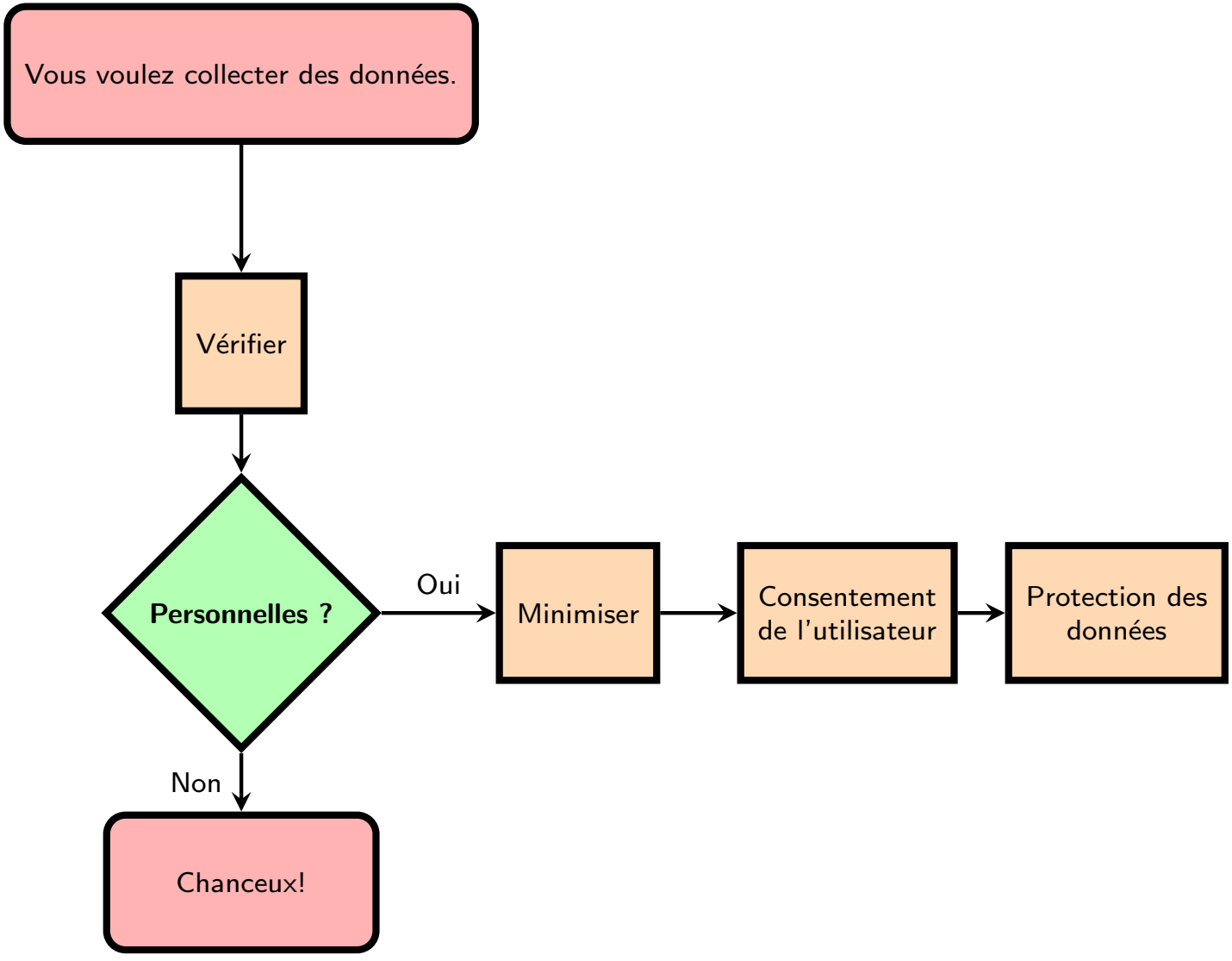
Cas d'étude 2 : Collecte de données



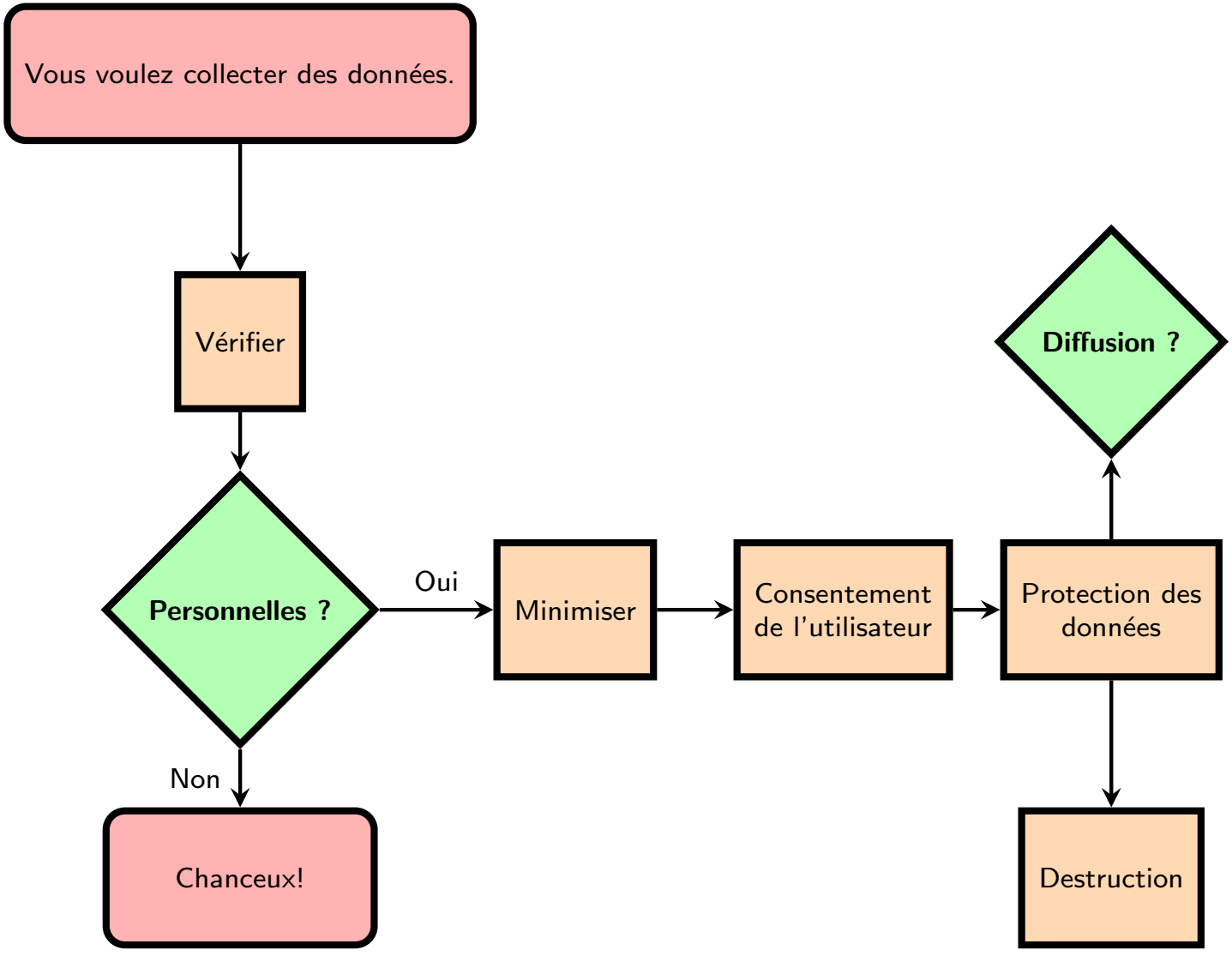
Cas d'étude 2 : Collecte de données



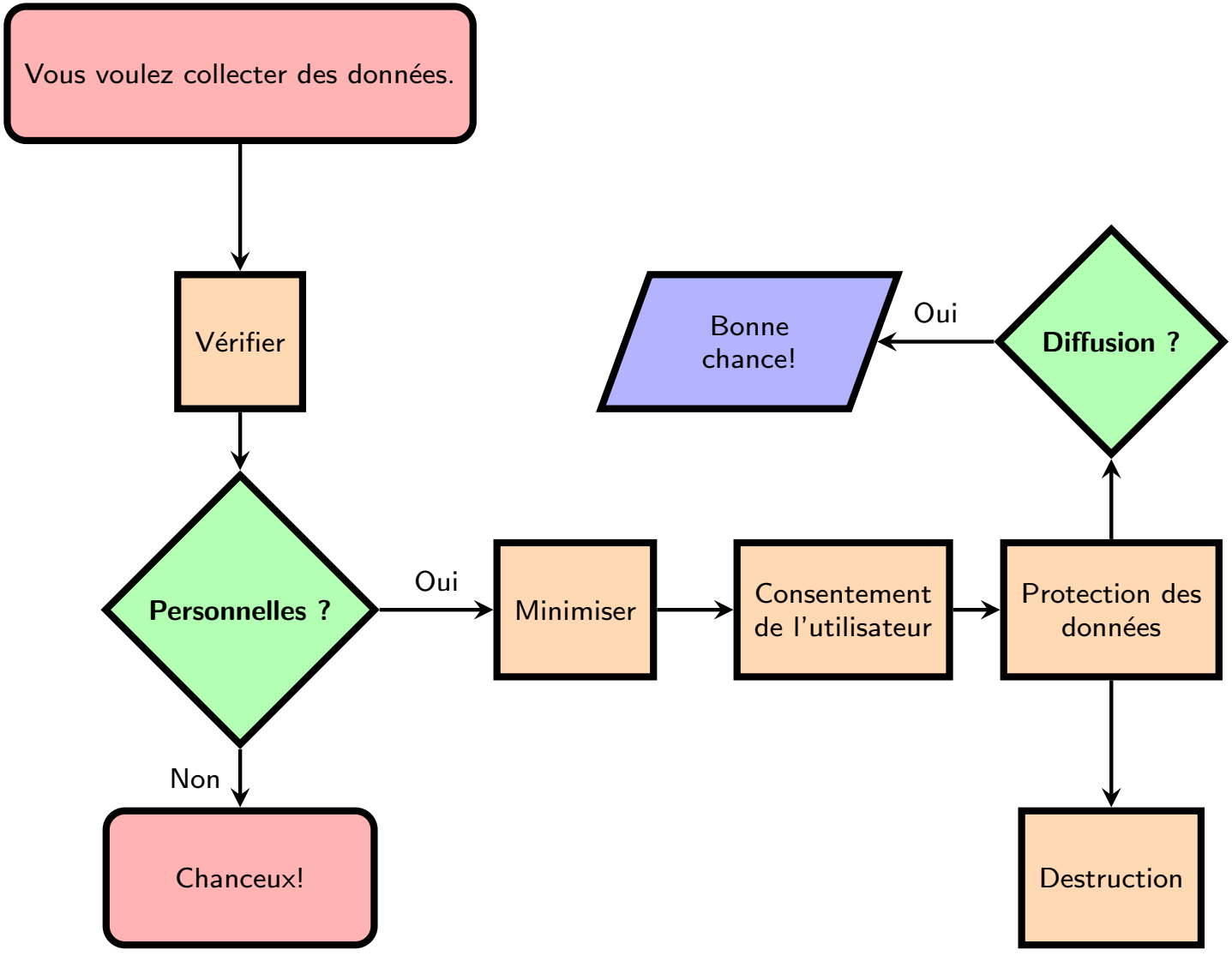
Cas d'étude 2 : Collecte de données



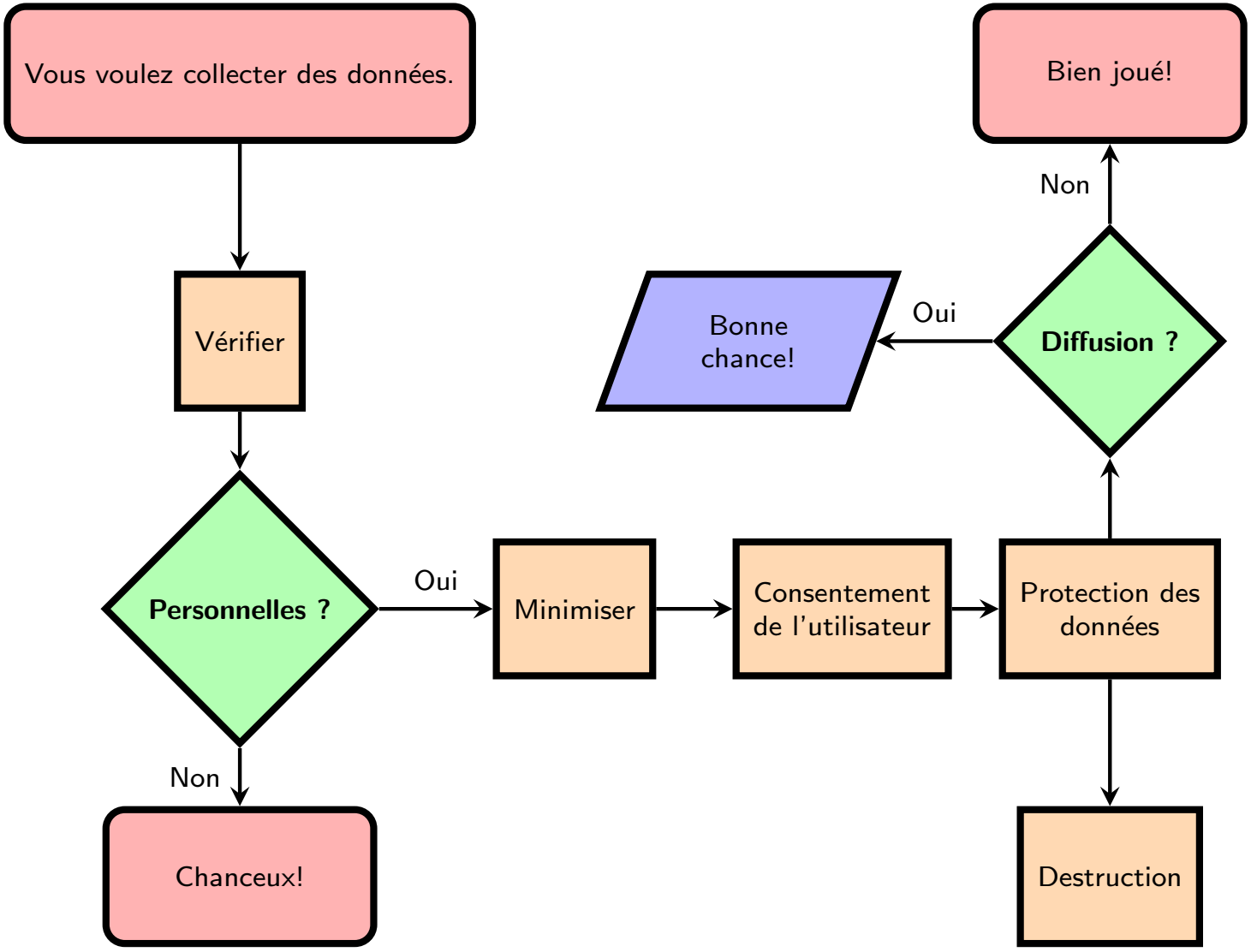
Cas d'étude 2 : Collecte de données



Cas d'étude 2 : Collecte de données



Cas d'étude 2 : Collecte de données



Qui doit être contacté ?

1. **Data Privacy Officer (DPO)**
   - Enregistrer les données collectées
   - Contacter les autoritées nationales (si nécessaire)
2. **Juriste**
   - Établir le formulaire de consentement
3. **Responsable de la Sécurité des Systèmes d'Information (RSSI)**
   - Mettre en place des outils pour protéger les données

Plan

Avant le 25 mai 2018

Après le 25 mai 2018

Conclusion

RGPD

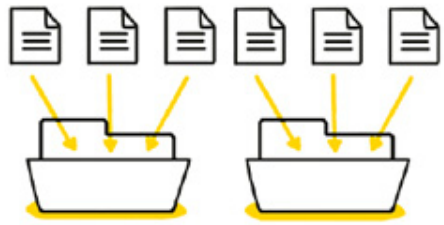
PASSER À L'ACTION

en 4 étapes

1

Constituez un registre de vos traitements de données

2



Faites le tri dans vos données

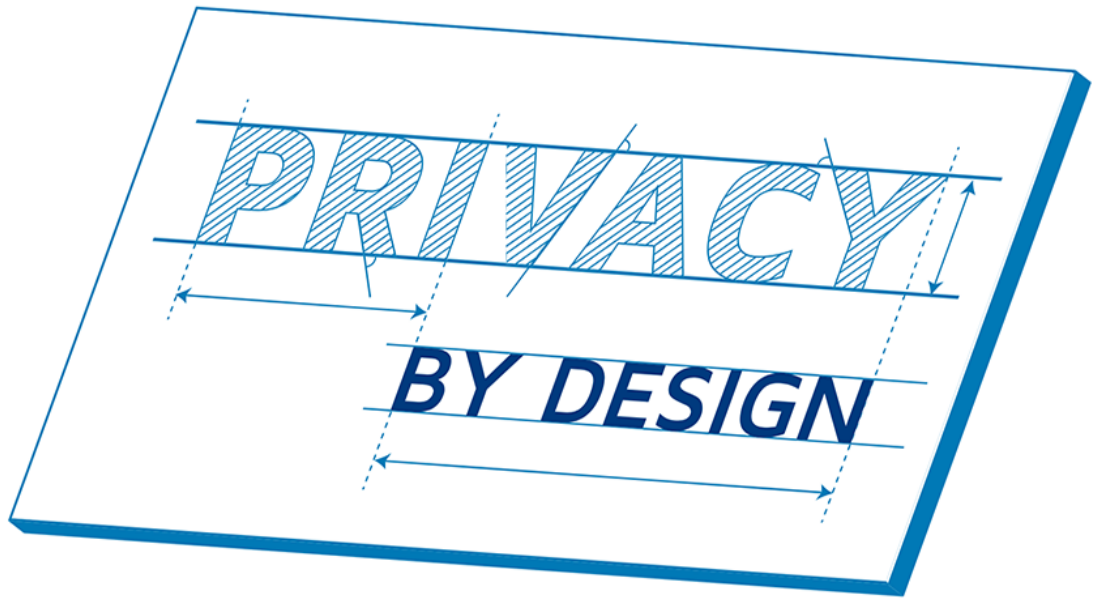
3

Respectez les droits des personnes

4

Sécurisez vos données

RGPD



Questions ?