RGPD

Assurer sa mise en conformité

SMILE
I.T IS OPEN

Faïza ZIANE
Hadrien GORMAND

1. **INTRODUCTION :** Rappels et définitions
2. **LA MÉTHODE SMILE :** Explications et principes : Smile est sous-traitant
3. **EXEMPLE D'UN CLIENT E-COMMERCE :** Application de la méthode Smile pour le RGPD
4. **ET SI ON INVERSAIT LES RÔLES :** Quand Smile se retrouve dans la position de « Responsable de traitement ».
5. **POUR FINIR :** Et réussir la mise en conformité RGPD avec Smile

INTRODUCTION

Rappels et définitions

SMILE
I.T IS OPEN

PRÉFACE

Approuvé par 29 pays européens signataires, toutes les organisations et entreprises qui détiennent ou traitent des données personnelles de citoyens européens doivent donc s'y conformer.
Le règlement entre en application **le 25 mai 2018 .**

Focus sur la donnée personnelle via un nouveau cadre règlementaire : **Protection et Sécurité à la Une !**

Le RGPD crée le cadre : « Nous renforçons la **confiance**. »

La transformation digitale de la société se nourrit des informations personnelles des citoyens (tracking, applications mobiles, objets connectés ,etc.). Or les citoyens sont de plus en plus sensibles à leurs libertés et à leurs données personnelles.

Le RGPD restitue par le droit, le pouvoir aux individus sur leurs données personnelles.

L'Europe a construit un instrument **unique** qui structure et impose des règles. L'annonce de sanctions envoie un signal fort, notamment aux GAFA (Google, Amazon, Facebook, Apple) : « Vous pouvez user des données personnelles, mais selon nos règles ! ».

MAIS, QU'EST CE QU'UNE DONNÉE PERSONNELLE ?

Selon l'article 2 du règlement :
« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres …. ».

"La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement".

Par exemple, une personne est identifiée lorsque son **nom** apparaît dans un fichier et aussi, par les données suivantes :

- Immatriculation
- Localisation
- Numéro de sécurité sociale
- Adresse électronique
- Date de naissance
- Informations de paiement
- Numéro de téléphone
- Empreinte
- Etc.

DONNÉES PERSONNELLES SENSIBLES

La loi distingue certaines données personnelles, comme des données « sensibles ». Elles font l'objet de dispositions particulières :

- Données génétiques ou biométriques
  - Données médicales
- Sanctions administratives ou suspicions
- Opinions politiques,
- Orientations sexuelles,

Petit rappel : en France, la collecte des données suivantes est particulièrement encadrée (loi de 1978) :

- Origine raciale ou ethnique
- Appartenance religieuse
- Appartenance syndicale

LA LOI EN BREF

1 Nouveau Règlement

29 pays signataires

25 Mai 2018, date d'entrée en application

4 % du CA global

ou 20 M€ d'amende

Le RGPD, obligations et opportunités :

- **Renforcer les droits des personnes**,
- **Harmoniser et unifier la législation** au sein de l'UE
- **Responsabiliser les acteurs** traitant des données et distinguer les « Responsables de traitement » et les « sous-traitants » ;
- Crédibiliser la régulation grâce à **une coopération renforcée entre les autorités de protection des données**, qui pourront notamment adopter des décisions communes et des sanctions renforcées, lorsque les traitements de données seront transnationaux.
- La nouvelle loi introduit **le droit au recours collectif** par le biais d'associations de consommateurs.
- Les transferts de données **hors UE** sont possibles dans la mesure où ils sont réalisés avec **des outils assurant un niveau de protection suffisant.**
  - D'autre part, les données transférées **hors Union Européenne restent soumises aux droits de l'UE** non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.

EXTENSION DES DROITS INDIVIDUELS

La nouvelle loi étend de 3 à 11 les droits individuels des citoyens

- Droit à une information complète sur le traitement des données exprimée de façon claire et simple
- Droit d'être informé en cas de violation de ses données personnelles
- Droit à l'oubli
- Droit à la limitation du traitement (pour faire valoir ses droits en justice)
- Droit à la portabilité des données (changement de fournisseur)
- Droit d'opposition (encadrement du profilage)
- Dispositions propres aux personnes mineures

QUI SONT LES ACTEURS RESPONSABLES DEVANT LA LOI ?

Le **Responsable de traitement**, selon l'article 4 du règlement, c'est :

- Toute personne physique, morale, l'autorité publique, le service ou un autre organisme, **qui détermine les finalités et les moyens** du traitement de données à caractère personnel.
- En d'autres termes, ce sont **les clients de Smile.**

Le **sous-traitant (ST)**, toujours selon l'article 4, c'est :

- Toute personne physique, morale, l'autorité publique, le service ou un autre organisme, **qui traite des données** à caractère personnel **pour le compte d'un responsable de traitement**.
- Exemples :
  - les prestataires de services informatiques (hébergement, maintenance, etc.)
  - les intégrateurs de logiciels, les sociétés de sécurité informatique
  - les entreprises de services du numérique (ESN) ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données
- En d'autres termes, **Smile fait parti de cette catégorie !**

LA LOI INTRODUIT DES SANCTIONS POUR LA PREMIÈRE FOIS

Des amendes pouvant atteindre
20 M€ ou 4%
du chiffre d'affaires global de votre organisation

Crédit photo : www.pexels.com

LA MÉTHODE SMILE

Explications et principes : Smile est sous-traitant

SMILE
I.T IS OPEN

COMMENT SMILE MET EN ŒUVRE LE RGPD ?

Smile a mis en place une démarche alliant processus et livrables

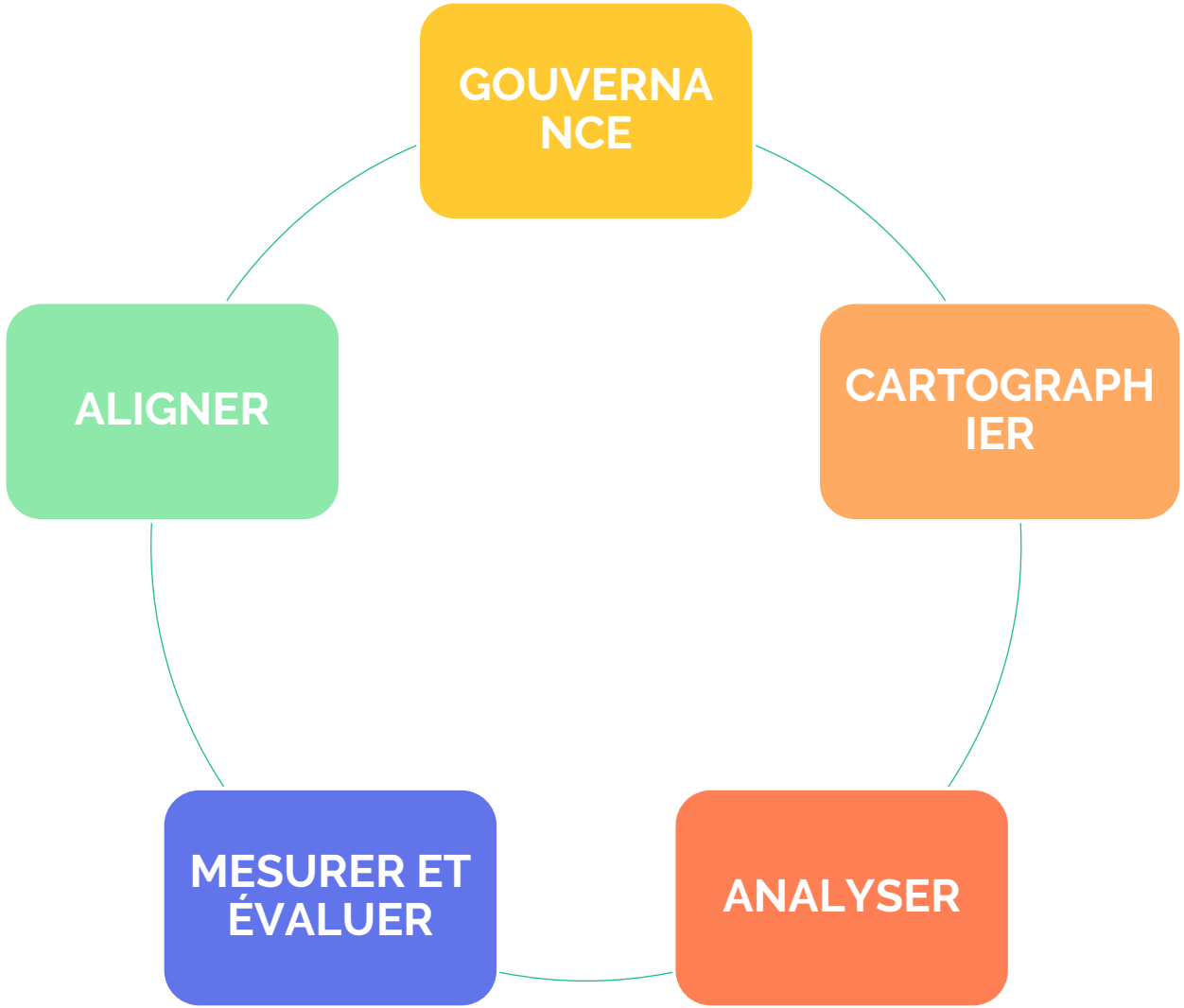
Afin de répondre aux nombreuses exigences du Règlement, dont le principe d'Accountability, les organisations (sous-traitant notamment) doivent démontrer les mesures globales qu'elles ont prises, notamment, afin d'assurer la traçabilité des informations.

La gouvernance et les usages des données deviennent centraux (maitrise des flux, exploitation, qualité, …) dans l'organisation mise en place.

Mais comment s'y prendre ?

- Smile préconise une démarche simple

DÉMARCHE & PROCESSUS



LES LIVRABLES DE LA MISE EN CONFORMITÉ RGPD

Premier livrable : **L'analyse de traitement**

- Cartographier les traitements de données personnelles, les flux.
- Créer le **registre de traitement** (recensement des traitements)
- Identifier les traitements indispensables et les traitements tiers
- Spécifier la finalité de chaque traitement
- Préciser pour chaque traitement les catégories de données, la durée, la volumétrie, les droits d'accès, etc.

Second livrable : **Evaluation de la protection des données**

- Les mesures à prendre en compte dans le respect des principes **"Privacy by design"** et **"Privacy by default"**
- Mesures organisationnelles (bâtiment protégé, …) et techniques
- Définition de la périodicité de test, d'analyse et d'évaluation

Troisième livrable : **Plan de mise en conformité**

- Plan détaillé par item et/ou fonction (Consentement, Purge, anonymisation, …)

PRIVACY BY DESIGN

PRIVACY BY DEFAULT

Concept visant à intégrer le respect de la vie privée **dès la conception**.

Il faut intégrer ce concept dès la phase d'analyse.

Intégrer le concept **« Privacy by design »** suppose que, dès le stade de la **conception d'un projet** intégrant des opérations de traitement de données personnelles, la **direction « métier »** concernée ait conscience que la technologie envisagée se doit de **respecter les principes** de protection des données (minimisation des données, pseudonymisation, etc.).

Cela signifie que la direction **« métier »** devra mettre en œuvre toutes les **mesures organisationnelles** et **techniques** appropriées afin que la technologie soit **conçue** et **développée** en conformité avec les exigences règlementaires.

Intégrer le concept de l'« **accountability** » suppose aussi que, dès le stade de la conception de la technologie, un processus et des dispositifs d'encadrement et de contrôle aient été mis en place. Pour permettre, à terme, à l'entreprise de pouvoir être en mesure de démontrer que les opérations de traitement réalisées au moyen de cette technologie sont en conformité avec les exigences règlementaires ; tous les processus devront avoir été de surcroît documentés.

ASSISTANCE DE SMILE AUPRÈS DU RESPONSABLE DE TRAITEMENT

L'engagement de Smile vis-à-vis du responsable de traitement :

- Le **notifier** dans le cas d'une violation de données dans les meilleurs délais (délais légaux)

- **L'assister** :
  - dans l'accomplissement de ses obligations en matière de sécurité et d'information ;
  - dans la réalisation d'une analyse d'impact sur son traitement
  - pour s'acquitter de ses obligations relatives aux droits des personnes (droit à l'effacement des données, droit d'accès, portabilité…)

- **L'informer** si l'une de ses instructions apparait susceptible de constituer une violation des règles imposées par le RGPD.

- **Apporter conseil** et **accompagnement** dans le cadre de la mise en œuvre du RGPD (démarche, processus , livrables)

EXEMPLE
UN CLIENT E-COMMERCE

Application de la méthode Smile
pour le RGPD

SMILE
I.T IS OPEN

ASSISTANCE DE SMILE AUPRÈS DU RESPONSABLE DE TRAITEMENT

Prenons un exemple parmi nos projets habituels

La plateforme e-commerce

- Une **plateforme e-commerce** peut collecter beaucoup de données personnelles.
- Smile assiste le responsable de traitement dans la mise en conformité RGPD.

Voici les étapes de mise en conformité RGPD que Smile met en œuvre pour accompagner son client e-commerçant :

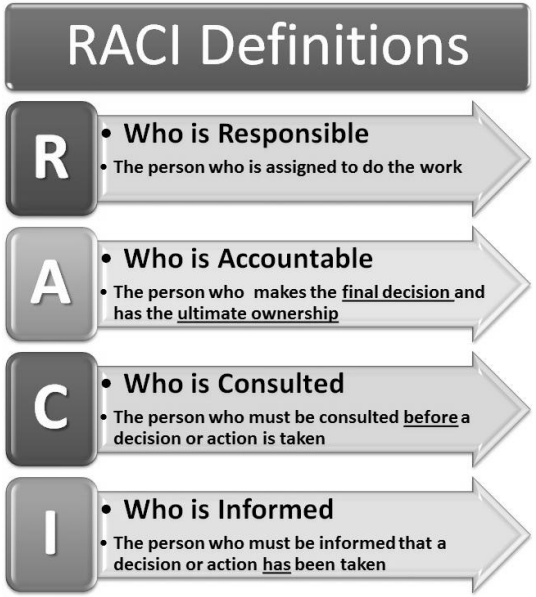
- 1. Gouvernance & processus
- 2. Cartographier
- 3. Analyser
- 4. Mesurer et Evaluer
- 5. Aligner : Plan de mise en conformité

Les pages suivantes vous détaille chaque étape.

ASSISTANCE DE SMILE AUPRÈS DU RESPONSABLE DE TRAITEMENT

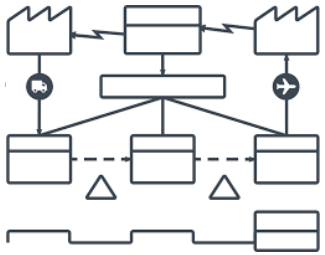
Etape 1 : Gouvernance & Process :

- Définir les acteurs :
  - le responsable de traitement, le client
  - le chef de projet ou consultant, Smile
- Définir et partager le R.A.C.I.
- Créer les outils documentaires



Etape 2 : Cartographier

- Créer le Registre de traitement
- Lister les traitements de données personnelles :
  - Par exemple : vente en ligne, facturation, livraison,
  - Mapping des flux internes/externes (par exemple prestataire de livraison)
- Définir les traitements indispensables et non indispensables
- Etc.



ASSISTANCE DE SMILE AUPRÈS DU RESPONSABLE DE TRAITEMENT

Lors du processus, les questions en amènent souvent beaucoup d'autres…

Etape 3 : Analyser

- Quelles sont les catégories de données personnelles collectées / traitées ?
  - Nom, prénom, email, …
- Qui sont les personnes concernées ?
  - Internautes par exemple
- Quelle est la durée de conservation de la donnée ?
  - Un compte client est inactif depuis 3 ans, doit on le conserver ?
  - Quelle est la durée de conservation d'une commande ?
  - Devons nous créer une base d'archive ?
  - Quelle est la fréquence de la purge ?
- Comment continuer à analyser le comportement des clients ?
  - Anonymisation des données ?
- Le déploiement du site est international
  - Comment s'applique le règlement pour les internautes hors UE ?
- Application du droit à l'oubli
  - Qu'en est il des prestataires tiers ?
  - Qu'en est il des commandes, des factures ?

Smile assiste ses clients et répond à toutes ces questions.

ASSISTANCE DE SMILE AUPRÈS DU RESPONSABLE DE TRAITEMENT

Smile développe des fonctionnalités

Elles sont intégrables selon des paramètres qui sont spécifiques au projet :

- Gestion des consentements
- Droit à l'oubli
- Anonymisation
- Purge
- Portabilité
- Chiffrement
- Etc.

4. Mesurer et Evaluer

- Evaluer le niveau de risque
- Intégrer le « **Privacy by design** »
- Établir les **mesures organisationnelles** (tous prestataires confondus y compris hébergement et exploitation)
  - chiffrement du stockage ou des bases de données
  - authentification forte pour les connexions aux serveurs
  - …
- Définir le **plan de sécurisation** des données **en transit**

5. Aligner : Plan de mise en conformité

- Items détaillés
  - Fonctionnalités produit
  - Actions techniques détaillées (hash, développement, …)
  - Création et mise à jour des processus (Violation des données, …)
- Actions par acteur cf. R.A.C.I.
- Planning de déploiement

Smile crée le plan de mise en conformité à vos côtés !

ASSISTANCE DE SMILE AUPRÈS DU RESPONSABLE DE TRAITEMENT

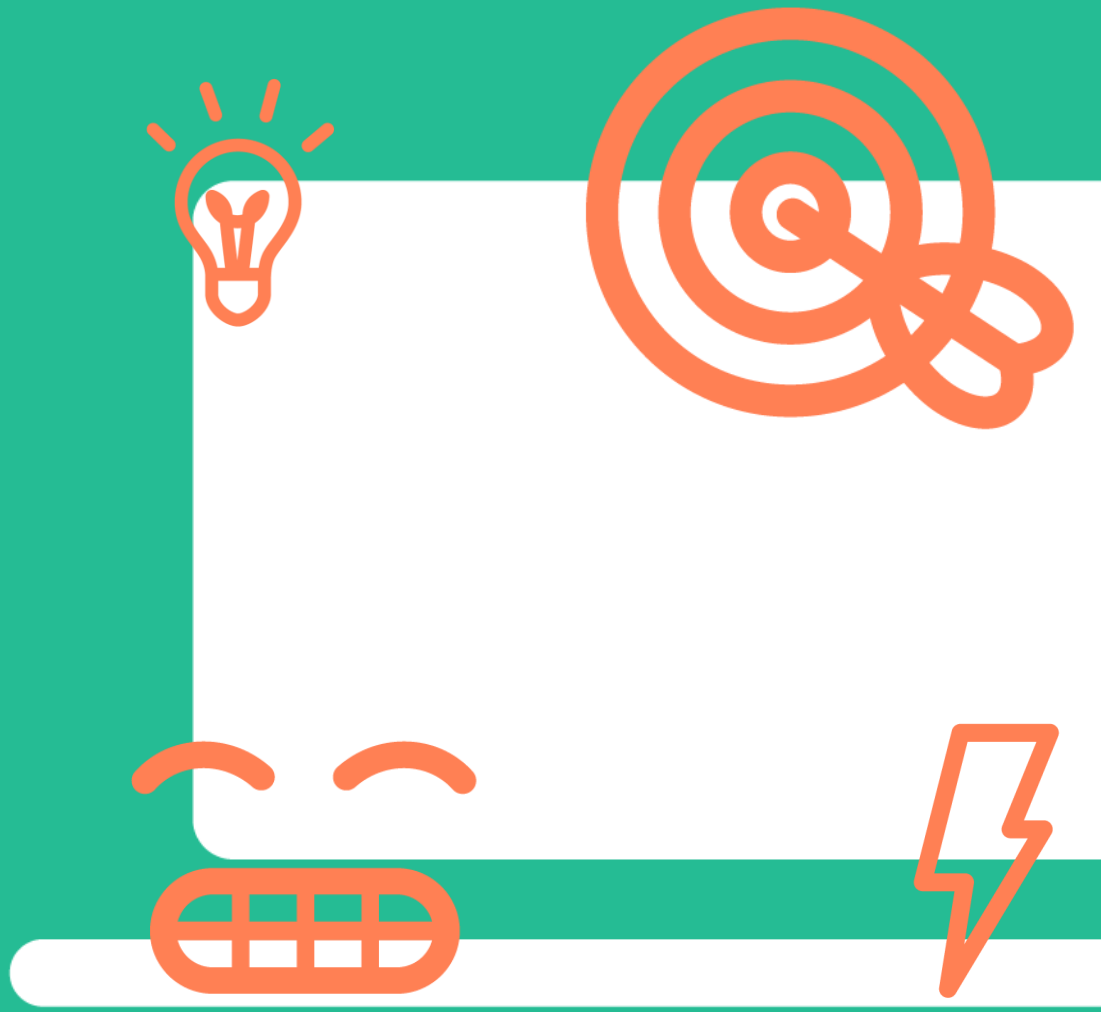
Plan de mise en conformité renforcé par la certification ISO/CEI 27001 de Smile en tant qu'hébergeur infogérant.

Overview des mesures de sécurité

Organisationnelles	• Mise en place d'un système de management de la sécurité, • Politiques de sécurité de l'information, • Définition d'objectifs et de responsabilité en matière de sécurité
Humaines	• Gestion des droits, des accès, du personnel • Formation & sensibilisation, etc.
Techniques	• Protection des accès, pare-feu, • Sondes de supervision • Mises à jour des systèmes • Outils de sécurité, etc.
Documentation et procédures de sécurité	• Gestion des incidents, • Gestion des actifs et des changements, • Veille sur les vulnérabilités, …
Autres exigences	• Plan de reprise d'activité • Gestion et revue des fournisseurs • Protection physique des centres d'activité et des zones d'hébergement • Plans d'audits, norme et son annexe,…

ET SI ON INVERSAIT LES RÔLES ?

Quand Smile se retrouve dans la position de « Responsable de traitement ».



SMILE
I.T IS OPEN

OBLIGATIONS DE SMILE EN QUALITÉ DE RESPONSABLE DE TRAITEMENT

OK

1. OBLIGATION DE TRANSPARENCE ET DE TRAÇABILITÉ

- Etablir un contrat avec ses clients
- Y recenser les traitements de données
- Autorisation du client en cas de sous-traitance
- Mise à disposition des informations pour démontrer que le sous traitant respecte ses obligations
- Tenir un registre de traitement

2. OBLIGATION DE PRENDRE EN COMPTE LES PRINCIPES DE PROTECTION DES DONNÉES

- Privacy by design
- Privacy by default

3. OBLIGATION DE GARANTIR LA SÉCURITÉ DES DONNÉES

- Collaborateurs soumis à la confidentialité
- Suppression et renvoi des données

4. OBLIGATION DE NOTIFICATION, D'ASSISTANCE ET D'ALERTE

- Violations de données
- Assistance et support au client :
  - demandes de droits d'accès et de suppression
  - Analyse d'impact
  - Conseil

DISPOSITIF SMILE EN QUALITÉ DE RESPONSABLE DE TRAITEMENT

Politique de protection des données	• Respect des principes énoncés dans le RGPD • Engagement de Smile de porter cette politique à la connaissance de ses clients
Délégué à la protection des données (DPD ou DPO)	• Désignation d'un DPD • Connaissances juridiques, pratiques en matière de protection des données • Garantie de contrôle, pilote de mise en conformité
Registre des traitements	• Etablissement de registre de traitement • Mise en place du processus et automatisation
Analyse de conformité des traitements	• Mise en place du modèle d'analyse des traitements • Procédure, pilotage et contrôle • Analyse des risques
Gestion des réclamations et des incidents	• Procédure de traitement des réclamations et des demandes • Procédure de notification

POUR FINIR

Et réussir la mise en conformité RGPD
avec Smile

SMILE
I.T IS OPEN

MISE EN CONFORMITÉ RGPD

Avec Smile, bénéficiez d'**un véritable diagnostic opérationnel** pour vous appuyer sur un plan d'actions

Smile vous accompagne !

- **Auditer** les systèmes d'information afin de déterminer le niveau de conformité, et formaliser les besoins et les écarts.
- Préparer un **programme de mise en conformité** et préconiser les mesures à mettre en œuvre pour assurer une conformité aux exigences légales et réglementaires
- Proposer **la mise en œuvre ou l'amélioration d'outils**, de **documents** de références internes et de **procédures de sécurité** adéquats.
- Procéder à la **rédaction de spécifications fonctionnelles**
- **Suivre la mise en œuvre** des nouvelles procédures et outils, et **former** à leur utilisation et **vous accompagner** au déploiement

MAIS QUI SOMMES-NOUS ?

SMILE

I.T IS OPEN

Avec de l'audace et des beaux projets, ajoutez une pincée de culture visionnaire, une bonne dose d'innovation, saupoudrez le tout d'une expertise technique pluridisciplinaire et vous obtenez **Smile, le leader européen de l'intégration et de l'infogérance de solutions open source**.

25
années d'expérience

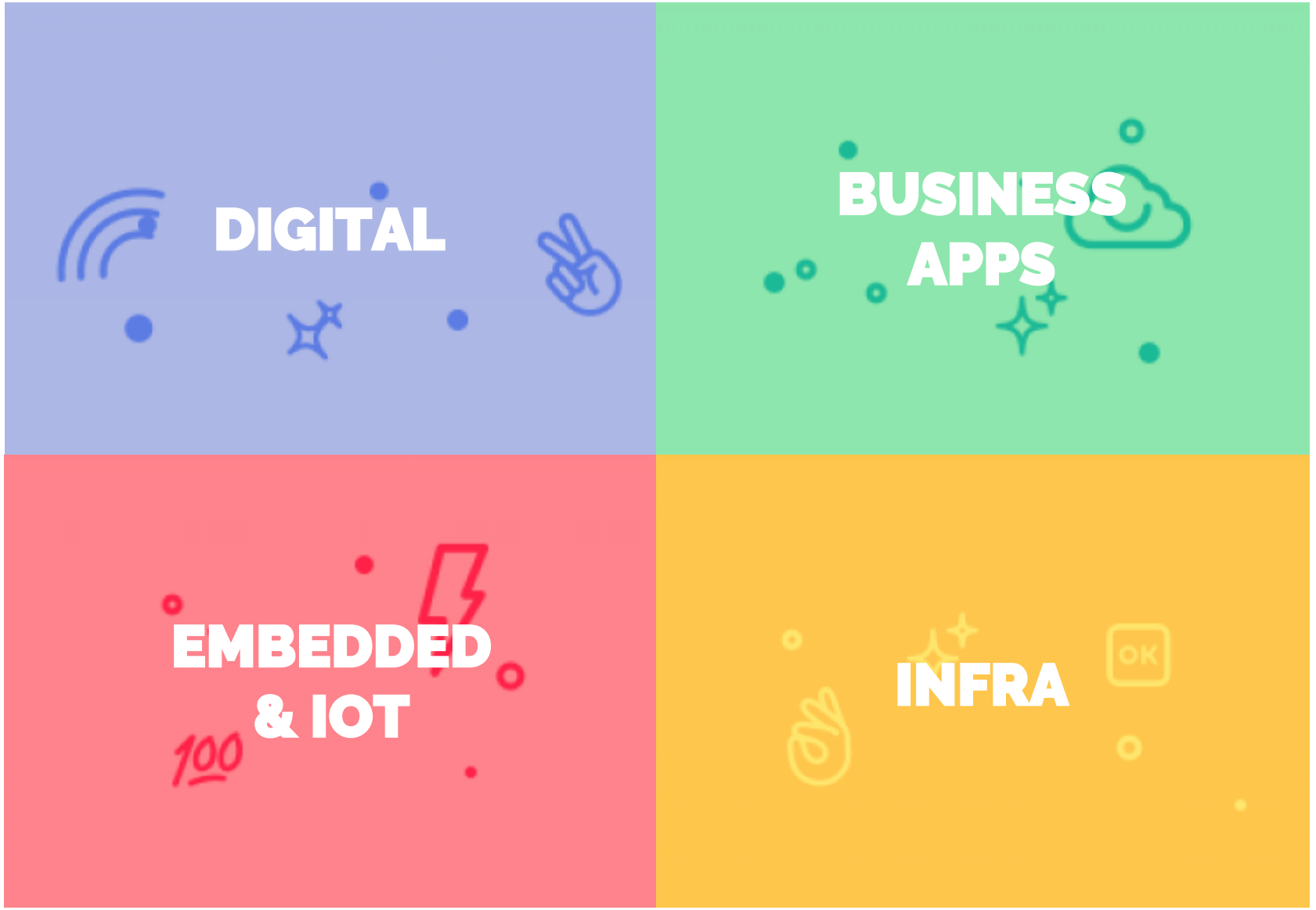
1200
collaborateurs

75
millions d'euros de CA en 2016

18
agences en France et à l'international

NOTRE OFFRE GLOBALE

Agiles, open et engagés, chez Smile, nous adorons avoir un coup d'avance pour garder notre place sur le podium des acteurs majeurs du digital. Pour cela, nous avons **développé 4 offres** pour vous accompagner dans votre transformation numérique



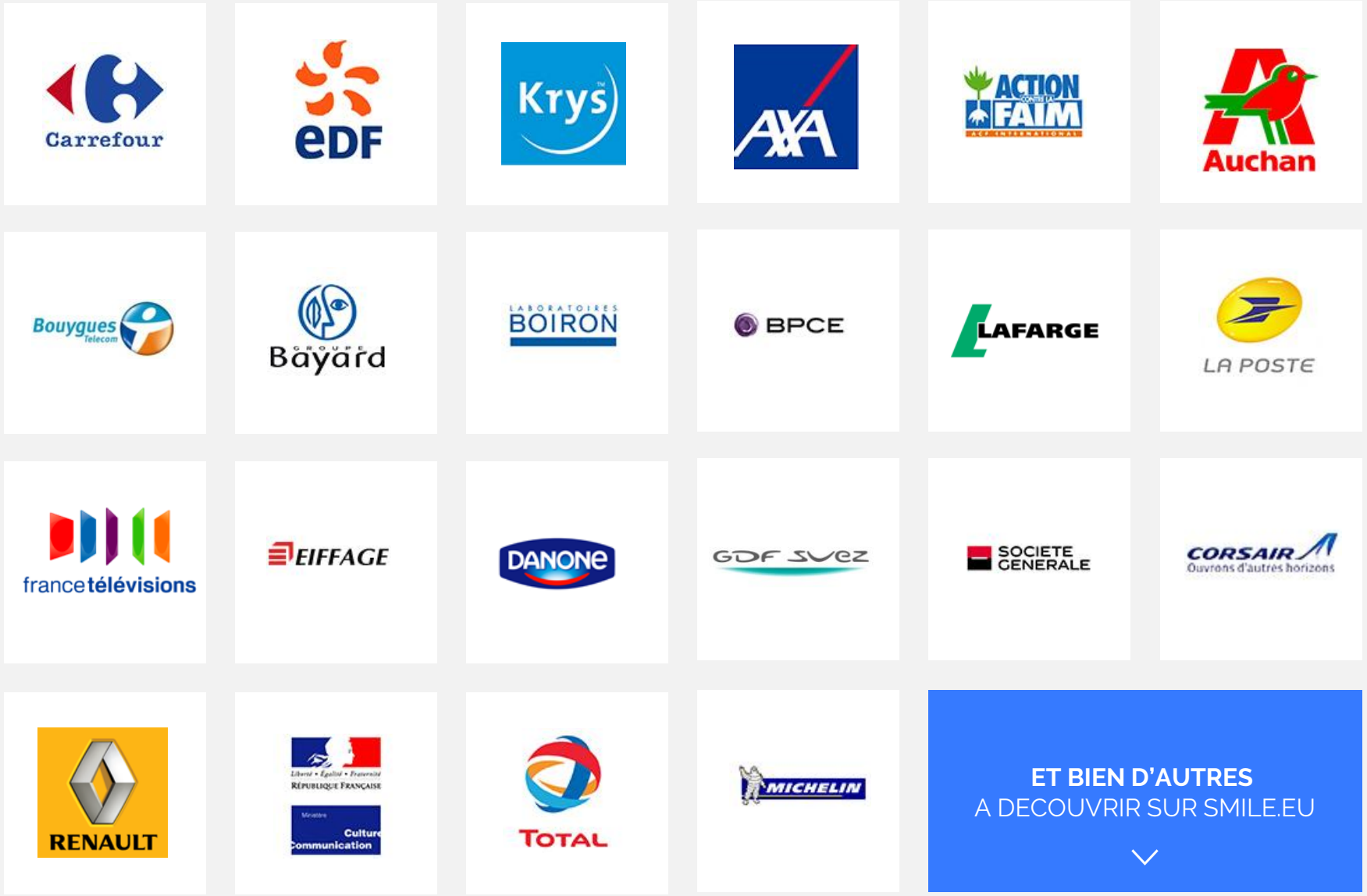
NOTRE ESPRIT DE PARTAGE

Notre collection de livres blancs vous accompagnera pas à pas dans la mise en place de vos stratégies digitales.

Téléchargeables gratuitement, ils vous présentent les concepts fondamentaux, les bonnes pratiques et les meilleures solutions open source du marché, sur les différents domaines d'expertise de Smile.

ILS NOUS FONT CONFIANCE

Toujours en quête de nouveaux challenges, nous sommes fiers d'accompagner au quotidien de nombreuses entreprises dans leurs projets de transformation digitale.



ET BIEN D'AUTRES
A DECOUVRIR SUR SMILE.EU

UNE QUESTION ? UN PROJET ? CONTACTEZ-NOUS !

Vincent Bourbon

Sales Development Manager

vincent.bourbon@smile.fr

01 41 40 59 31

www.smile.eu