



Centre d'Information sur les Médias A.S.B.L.
Centrum voor Informatie over de Media v.z.w.

CIM Internet

Information sur la gestion du consentement

Version 24 novembre 2022

Tableau des matières

1. Introduction.....	2
2. Gestion du consentement.....	3
3. Clause de non-responsabilité en matière de confidentialité	5
4. Politique des cookies.....	7
5. Partenaires	9
6. Résumé.....	10
7. Références et sources	11

1. Introduction

L'utilisation de cookies sur internet est réglementée (entre autres) par la Directive « Vie privée et communications électroniques » (e-Privacy Directive), telle que mise en œuvre par les états membres de l'UE, et le Règlement Général sur la Protection des données (RGPD).

Des décisions récentes de la Cour Européenne de Justice ainsi que des lignes directrices émises par le Comité Européen de la Protection des Données offrent des directives quant à leur interprétation. La conclusion est simple : sans consentement de l'utilisateur, le placement de cookie est interdit (à quelques exceptions près).

Ce principe a inspiré les organisations professionnelles digitales, les fournisseurs de services et les autorités en charge du respect de la vie privée :

- L'IAB Europe a développé un ensemble de normes spécifiques au secteur pour la collecte et la diffusion du consentement dans la pratique, pour le marketing digital sous le Transparency and Consent Framework (TCF). Une partie de ce cadre est une classification des finalités des cookies et autres identifiants, des fonctionnalités et du traitement des données (voir Tableau 2, Chapitre 4) qui peuvent être agrégés ou simplifiés par les propriétaires de sites.
- Les fournisseurs de plateformes de gestion du consentement (Consent Management Platform – CMP) aident les éditeurs à donner aux utilisateurs le moyen de contrôler les identifiants sur leurs appareils et à sélectionner les finalités et les fonctionnalités qu'ils sont prêts à accepter. Cela permet aux éditeurs de développer leurs services dans le respect des préférences des utilisateurs.
- L'Autorité Belge de la Protection des Données a tendance à appliquer et à interpréter les règles applicables de manière assez stricte.

Cette évolution du cadre juridique, ainsi que le refus croissant des cookies tiers par les internautes et les fournisseurs de technologie, ont eu une grande influence sur les politiques relatives aux cookies des sites internet. Néanmoins, alors que les cookies tiers sont amenés à disparaître, les éditeurs ont toujours l'obligation de mettre à jour leur politique des cookies et leur gestion du consentement pour répondre aux exigences légales actuelles.

La mesure CIM Internet utilise des cookies (tiers) depuis 2000. Inévitablement nos études sont adaptées aux changements climatiques dans le monde digital. Ce document propose des informations qui pourront aider les éditeurs à suivre les changements dans les identifiants, la Gestion du Consentement et la Clause de non-responsabilité en matière de confidentialité (Privacy Disclaimer). En tant que tel, il couvre différents éléments d'une politique des cookies conforme au RGPD. Le point de départ est l'interprétation par les autorités belges de la législation appropriée. Certaines recommandations s'inspirent des règles du Transparency and Consent Framework (TCF) de l'IAB Europe. Plusieurs souscripteurs de l'étude CIM Internet utilisent les standards du TCF de l'IAB, d'autres pas. Ce document a été rédigé pour être pertinent dans les deux cas.

Il doit être clair que les éditeurs sont les seuls responsables de la Gestion du Consentement, de la Politique des Cookies et de la Clause de non-responsabilité en matière de confidentialité sur leurs plateformes digitales. Il est facile de faire des erreurs ou d'oublier des éléments cruciaux. Suivre ce document ne garantit en aucun cas la conformité dans ces cas spécifiques. Nous recommandons donc aux souscripteurs de demander des conseils techniques et juridiques auprès d'experts.

2. Gestion du consentement

L'utilisateur doit activement donner son consentement pour tous les identifiants non-essentiels, et ce sur une base suffisamment informée. Ce n'est qu'alors que les identifiants non-essentiels peuvent être placés dans le navigateur de l'utilisateur lors de la visite du site. Toute modification du consentement de l'utilisateur doit entraîner le transfert ou non-transfert des identifiants.

L'étude CIM Internet mesure l'activité du navigateur et de l'app au moyen d'identifiants fournis ou collectés par Gemius. Ces identifiants ne sont pas essentiels et nécessitent le consentement des utilisateurs avant leur transfert.

La gestion du consentement doit être conforme aux principes suivants :

1. L'activation de identifiants non-essentiels n'est autorisée qu'après consentement
Dans le cadre de l'étude CIM Internet, cela signifie que les identifiants ne peuvent être transmis qu'après consentement. Le règlement de l'étude CIM Internet traduit ce principe en exigences pratiques dans le cas où une plateforme de gestion du consentement (CMP) est utilisée, et précise l'action requise dans le cas où l'utilisateur refuse son consentement alors qu'aucune CMP n'est utilisée.
2. Consentement éclairé
Pour les identifiants qui nécessitent le consentement de l'utilisateur, il doit se voir proposer un choix clair et éclairé. Cela peut se faire de différentes manières :
 - La première approche consiste à définir l'option de désactivation (opt-out) par défaut.
 - La deuxième approche affiche les deux options, sans privilégier l'une par rapport à l'autre.
 - Une troisième approche consiste à définir l'option d'activation (opt-in) par défaut en suggérant que cette option-là est l'option logique ou la bonne option à choisir. Veuillez noter que cette approche est fortement déconseillée et critiquée par certaines autorités de protection des données.

La **deuxième approche**, comme présentée dans le Tableau 1, minimise le risque de discussion sur la conformité au RGPD.

Tableau 1. Aperçu des approches pour demander l'activation (opt-in) des utilisateurs.

Approach 1	Approach 2	Approach 3
Intro text on use of cookies	Intro text on use of cookies	Intro text on use of cookies
Agree Opt out	Agree Opt out	Agree Opt out

3. Disponibilité des informations spécifiques sur les identifiants
Les utilisateurs intéressés doivent pouvoir trouver facilement des informations supplémentaires sur les identifiants utilisés :
 - Leur finalité,

- Le type de traitement des données rendu possible par un cookie spécifique,
- Et sa durée de vie.

La liste des finalités des identifiants utilisés dans l'étude CIM Internet est plus limitée que celle attribuée à Gemius dans le cadre du TCF v1 ou 2 de l'IAB. Le script a été adapté pour que les cookies ne soient utilisés que pour les finalités appropriées pour l'étude.

Outre ces 3 exigences, les éléments suivants méritent d'être pris en compte :

1. L'utilisation des pop-ups de consentement

Des recherches montrent que le pouvoir d'arrêt et le pouvoir d'activation des pop-ups sont très efficaces.

Le pop-up apparaît comme une couche au-dessus du contenu et invite l'utilisateur à donner son consentement ou refus pour les identifiants. L'utilisateur comprend directement qu'un opt-in ou opt-out actif est nécessaire avant de pouvoir accéder au contenu du site.

Le pop-up doit contenir un lien cliquable vers des informations plus spécifiques sur les identifiants utilisés et la Clause de non-responsabilité en matière de confidentialité.

Les sites qui n'ont pas de pop-up doivent s'assurer que les surfeurs:

- disposent de toutes les informations correctes relatives au traitement de leurs données ;
- ont la possibilité d'accepter ou refuser l'utilisation des identifiants Gemius dans le cadre l'étude CIM Internet.

2. L'utilisation d'une plateforme de gestion du consentement (CMP) sur les sites et dans les apps qui utilisent des pages Webview.

Une CMP invite les utilisateurs à donner leur consentement, centralise l'échange d'informations de consentement et structure ces informations dans un Transparency Consent String (TCF).

Une CMP peut être développée par le propriétaire du site internet ou en partenariat avec un fournisseur de CMP (Didomi, Sourcepoint, OneTrust, Usercentrics, etc.). L'IAB Europe propose une liste de fournisseurs de CMP enregistrés ([registered CMP providers IAB](#)). Cette information doit faire partie de la Clause de non-responsabilité en matière de confidentialité et sera traitée dans un chapitre séparé de ce document.

3. L'utilisation du IAB TCF v2.0.

Ce cadre aide les éditeurs à gérer le consentement des utilisateurs de manière conforme au RGPD. Les paramètres et l'utilisation proposée du Transparency Consent String permet d'apporter de la transparence et de la responsabilité. L'IAB publie également la liste internationale des fournisseurs (Global Vendor List) reprenant les partenaires conformes au RGPD et le type d'utilisation des identifiants qu'ils peuvent généralement proposer. Les éditeurs peuvent utiliser les informations de cette liste, ou faire référence à la liste, sur leurs propres sites internet.

La CMP fournit plusieurs niveaux d'informations aux utilisateurs d'un site, notamment la liste des partenaires. La présence d'un symbole IAB pour certains partenaires indique qu'ils sont enregistrés et certifiés par l'IAB. Pour ceux-ci, les informations (telle que la liste des finalités des identifiants) sont fournies automatiquement.

Toutefois, cette liste des finalités fournie pour Gemius en tant que fournisseur certifié par l'IAB est plus large que la liste des finalités applicables en réalité pour l'étude CIM Internet. Le CIM examine auprès des différents fournisseurs de CMP s'il est possible d'indiquer Gemius comme partenaire IAB avec uniquement les finalités de l'étude.



Pour l'instant, supprimer Gemius de la liste des fournisseurs IAB affichée dans le CMP n'est pas une solution car le script doit y faire référence pour fonctionner correctement.

4. L'absence de pop up ou de CMP

Les sites qui n'utilisent pas de CMP doivent s'assurer que le consentement (ou refus) des surfeurs soit enregistré de manière à être communicable au script de Gemius.

Aucun identifiant n'est transmis si l'utilisateur n'a pas donné son consentement. Dans ce cas-là, le script de mesure Gemius envoie des hits sans cookies. Ces hits sans cookies permettent une mesure anonyme du trafic : nous comptons les pages vues sans identifier ni suivre les utilisateurs à travers un site. Avec ce volume, nous connaissons la totalité du trafic, ce qui permet d'estimer plus précisément le nombre d'utilisateurs "réels". Sans ce volume, la mesure du trafic et de l'audience est sous-estimée.

Les éditeurs sont responsables de l'implémentation de toutes les variables nécessaires dans le script de mesure Gemius (conformément aux instructions fournies par le CIM) pour assurer l'envoi de hits sans cookies lorsqu'ils ont été refusés par les utilisateurs.

3. Clause de non-responsabilité en matière de confidentialité

La clause de non-responsabilité en matière de confidentialité décrira la politique de l'éditeur sur les Données Personnelles en termes concis, précis et faciles à comprendre. Plusieurs éléments doivent être mentionnés, comme l'utilisation des identifiants, et spécifiquement ajustés à l'étude CIM Internet.

La clause de non-responsabilité en matière de confidentialité fera également référence, de la manière la plus claire possible, au droit de l'utilisateur d'exercer ses droits RGPD.

3.1. Politique relative aux données personnelles

La politique relative aux données personnelles doit couvrir les sujets suivants.

1. Une identification claire de l'éditeur responsable des données.
2. Des informations de contact pour les internautes qui souhaitent poser des questions au sujet des données personnelles ou qui veulent exercer leurs droits relatifs au RGPD. Et si elles sont disponibles, les coordonnées du DPO.
3. Les finalités pour lesquelles les données sont collectées. Pour chaque finalité :
 - quels types de données sont collectés,
 - à quels fins les données sont utilisées,
 - combien de temps les données sont stockées.
4. La base juridique ou l'intérêt légitime pour la collecte et le traitement des données à caractère personnel.
5. Le droit de retirer son consentement avec une référence sur la manière de le faire.
6. La mention des parties tierces auxquelles les données à caractère personnel sont transmises, y compris les codes utilisés pour la collecte des données par ces parties tierces.
7. Si applicable, la spécification de la responsabilité conjointe des données. La répartition des rôles et les coordonnées des parties impliquées. Notez que les technologies tierce mises en œuvre pour collecter les données impliquent une responsabilité partagée des données.

8. En cas de transfert de données en dehors de l'UE, toutes les informations requises pour protéger les données à caractère personnel.
9. Des informations sur l'utilisation, la finalité et la durée de vie des identifiants, y compris les cookies tiers avec la référence aux partenaires correspondants.
10. Des informations sur l'application possible de certifications ou codes de conduite (y compris TCF) pertinents.
11. La mention de la collecte des données pour des décisions automatisées. Des techniques de décisions automatisées peuvent être utilisées pour profiler de la publicité ciblée et contextualisée, du marketing de contenu, etc. Par exemple, lorsque la publicité ciblée est basée sur des décisions entièrement automatisées, c'est-à-dire sans aucune implication humaine, l'impact juridique ou majeur doit être évalué en prenant en compte des critères comme le caractère intrusif du processus de profilage et la vulnérabilité particulière des sujets ciblés. En cas d'impact juridique ou majeur, le sujet doit avoir le droit de s'opposer à faire l'objet des décisions uniquement automatisées.

Un lien direct vers la page sur la clause de non-responsabilité en matière de confidentialité doit être disponible dans le pop-up mais aussi accessible depuis n'importe quelle page d'un site (souvent au bas de la page).

Toutes les informations relatives aux identifiants et au traitement des données peuvent être intégrées ou détaillées dans la Politique des cookies, mentionnée dans la Clause de non-responsabilité en matière de confidentialité.

3.2. Exercice des droits des utilisateurs

Le RGPD définit les droits pouvant être exercés par les utilisateurs. Ceux-ci doivent en être clairement informés. Pour ce faire, le texte ci-dessous, en anglais, peut être utilisé comme source d'inspiration.

1. You have the right to refuse consent to the use of cookies and all personal data processing for which your consent is needed.

2. If you have given your consent, you can withdraw your consent at any time. Your revocation will not affect the legality of the treatment made before your revocation of your consent. For the use of cookies, this can be easiest done by deleting your cookies ([instructions](#)).

3. You have the right to access and to receive a copy of all the personal information which the data controller may have registered about you. It can, for example, be your contact information and registrations for our events. Queries can be sent to: [\[insert relevant e-mail address\]](#).

4. You have the right to have incorrect information about you corrected. If our registered information is incorrect, we will gladly correct it. Corrections can be sent to: [\[insert relevant mail address\]](#).

5. You have the right to opt out of profiling and direct marketing.

6. You have the right - for reasons relating to your personal situation - to object against the processing of your personal data that we make based on our legitimate interest. However, the objection may be rejected if the data controller can prove weighty legitimate reasons for



the treatment that take precedence over your interests, rights and liberties, or the processing is necessary for the determination of a legal claim, asserted or defended.

7. In certain cases, you have the right to object to have your personal data processed. If you have the right to have your information restricted, we may in future - in addition to storage - only process the information with your consent or for the purpose that a legal claim can be established, asserted or defended to protect one person or important societal interests.

8. In special cases, you have the right to have information about you deleted before the time of our common general deletion occurs. For example, if the information is no longer available relevant to the purpose for which they were collected.

9. You have the right to data portability. That is, to have your personal information transmitted in a structured, commonly used and machine-readable format, as well as having your transferred personal data from one data controller to another. However, this only applies to data that you itself has submitted by automatic means (i.e. not paper documents), and which are processed on the basis of consent or contract.

4. Politique des cookies

Dans le cadre du RGPD, l'utilisateur doit être clairement informé de la finalité et de la fonctionnalité des identifiants, la durée de vie s'il s'agit de cookies ainsi que du type de traitement de données qu'il permet, par le biais d'une politique des cookies (intégrée dans la Clause de non-responsabilité en matière de confidentialité, ou qui y est mentionnée).

Une première distinction peut être faite en fonction du caractère essentiel de l'identifiant. Les identifiants à caractère non-essentiel nécessitent un consentement préalable. Les identifiants Gemius utilisés dans l'étude CIM Internet ne sont pas essentiels car ils n'influencent d'aucune manière le fonctionnement du site internet ni l'expérience de l'utilisateur.

Les identifiants non-essentiels peuvent se distinguer par leurs caractéristiques, le traitement des données et leur finalité. Il est important de noter que la finalité qui s'applique à un identifiant donné dépend d'une part des caractéristiques fonctionnelles de ce cookie mais aussi du contexte dans lequel le cookie est utilisé.

Dans le cadre de l'étude CIM Internet, les identifiants Gemius sont utilisés à des fins 'statistiques', tandis que ces mêmes identifiants Gemius peuvent servir à d'autres fins, 'marketing' par exemple, dans d'autres études, pays ou contextes.

Afin d'aider les éditeurs et les fournisseurs de CMP à définir correctement les finalités des identifiants, l'IAB TCF v2.0 propose des paramètres par défaut permettant définir les finalités utilisées par chaque fournisseur d'identifiants.

Le tableau suivant reprend la liste des finalités, des fonctionnalités et des types de traitement identifiés par l'IAB. Ceux indiqués en **bleu** sont applicables aux identifiants Gemius utilisés dans l'étude CIM Internet.

Tableau 2. IAB TCF v2.0 Classification pour les identifiants

FINALITES, FONCTIONNALITES PARTICULIERES ET AUTRES	
Finalité 1.	Stocker des et/ou accéder aux informations sur un appareil
Finalité 2.	Sélectionner les publicités de base
Finalité 3.	Créer un profil publicitaire personnalisé
Finalité 4.	Sélectionner les publicités personnalisées
Finalité 5.	Créer un profil de contenu personnalisé
Finalité 6.	Sélectionner du contenu personnalisé
Finalité 7.	Mesurer les performances de la publicité
Finalité 8.	Mesurer les performances du contenu
Finalité 9.	Appliquer des études de marché pour générer des informations sur l'audience
Finalité 10.	Développer et améliorer des produits
Fonctionnalité particulière 1.	Utiliser des données de géolocalisation précises
Fonctionnalité particulière 2.	Scanner de manière active les caractéristiques des appareils pour identification
Autre.	Respecter les droits RGPD de se désinscrire et d'être oublié
TYPES DE TRAITEMENT DES DONNEES	
Type 1.	Faire correspondre et combiner les données
Type 2.	Etablir un lien entre plusieurs appareils
Type 3.	Recevoir et utiliser les caractéristiques des appareils envoyées automatiquement

Les éditeurs sont libres d'utiliser cette liste, de regrouper des finalités ou d'en ajouter d'autres, de la manière la plus appropriée pour leur site. Les éditeurs sont également libres de choisir la manière dont ils organisent ces informations : par ex. une liste de toutes les caractéristiques par cookie individuel ou une liste de tous les identifiants par type de finalité...

Par souci de clarté, le CIM invite les souscripteurs à organiser toutes les informations pertinentes sur les identifiants de l'étude CIM Internet en utilisant :

- Une convention de dénomination commune des différentes finalités.
- Un langage consommateur simple lors de la description de la finalité.
- Une catégorisation partagée des finalités spécifiques. Par exemple, certaines finalités appartiennent les unes aux autres et peuvent être regroupées et nommées dans une catégorie distincte.
- Une utilisation cohérente des noms, labels, groupes, descriptions, etc., chaque fois que sont présentées des informations sur les identifiants.

En plus de la finalité des identifiants, pour les cookies il est nécessaire de donner des informations quant à la durée de vie. Celle-ci doit être raisonnable et en proportion avec la finalité d'un cookie. Sauf quelques cookies spécifiques (p.ex. un membre actuel du panel ne doit plus être invité pour ce panel), le CIM envisage une durée de vie de 13 mois pour les cookies de l'étude CIM Internet. La durée de vie de certains cookies commence à partir de la dernière visite de l'internaute sur le site. Le CIM va justifier et documenter chaque changement afin que les souscripteurs puissent intégrer l'information correcte dans leur politique de cookies.

5. Partenaires

L'utilisateur a le droit de connaître tous les partenaires qui collectent, stockent ou reçoivent des informations (identifiants) du site internet qu'il visite. L'éditeur doit répertorier toutes ces parties tierces dans la Clause de non-responsabilité et dans la Politique de respect de la vie privée ou dans la Politique des cookies.

En général, cet aperçu doit au minimum inclure :

- Une identification précise du contrôleur des données pour chaque identifiant.
- Une liste de toutes les parties tierces impliquées.
Remarque : si une partie tierce souhaite traiter les informations sur base d'un intérêt légitime, cela doit être indiqué, tout comme le fait qu'il est toujours possible de s'opposer à ce traitement.
- Une description des finalités pour lesquelles les parties tierces concernées utilisent les informations.
- Un aperçu des identifiants, y compris la durée de vie s'il s'agit des cookies.

L'aperçu peut être organisé de manière à ce que les utilisateurs puissent donner leur consentement sous différents angles : par la (dé)sélection des finalités, la (dé)sélection des partenaires ou la (dé)sélection des identifiants.

En se référant aux partenaires et aux cookies correspondants utilisés dans l'étude CIM Internet :

- il doit être possible de faire des sélections et désélections individuelles pour chaque parties tierces et pour chaque finalité ;
- il doit être possible de faire des sélections et désélections individuelles pour chaque fonction spéciale ;
- toutes les options doivent être désactivées, et les utilisateurs doivent faire un opt-in actif pour une ou plusieurs finalités.

Les options suivantes peuvent faciliter le consentement de l'utilisateur.

- La possibilité de rechercher une partie tierce individuelle et d'enquêter sur les types des identifiants qu'elle utilise ainsi que la finalité correspondante.
- La possibilité de travailler dans l'autre sens et de rechercher toutes les parties tierces qui sollicitent le consentement pour une finalité précise, par ex. 'Développement de produit'.

Les Partenaires concernés par l'étude CIM Internet sont repris dans l'article 8 du règlement de l'étude CIM Internet. Il s'agit de Gemius et du CIM en tant que coresponsables du traitement (joint controllers) des identifiants Gemius utilisés.

6. Résumé

Les chapitres précédents indiquent clairement que le RGPD exige le respect des règles spécifiques qui doivent être correctement interprétées. La liste ci-dessous résume les exigences minimales que les éditeurs souscripteurs de l'étude CIM Internet doivent prendre en considération :

- Le transfert de l'identifiant du navigateur (Browser ID) et de tout autre futur identifiant non-essentiel utilisé dans l'étude CIM Internet n'est autorisée qu'après consentement de l'utilisateur ;
- Une plateforme de gestion du consentement permettant d'aligner l'échange de données personnelles avec le consentement de l'utilisateur ;
- Un pop-up qui informe l'utilisateur, lui demande son consentement de manière neutre et qui comporte un lien vers la Politique de respect de la vie privée et la Politique des cookies ;
- Toute Politique de respect de la vie privée doit inclure tous les éléments pertinents pour l'étude CIM Internet, comme spécifié dans le règlement de l'étude CIM Internet (version mise à jour disponible sur le site internet du CIM en [français](#) et en [néerlandais](#)) :
 - o la liste complète des identifiants liés à l'étude CIM Internet,
 - o avec des informations identifiant par identifiant sur le type et les finalités,
 - o la durée de vie s'il s'agit des cookies.

Vous pouvez intégrer ces éléments dans votre propre Clause de non-responsabilité en matière de confidentialité ou faire référence vers le [CIM Privacy Disclaimer](#) (comme c'est déjà le cas actuellement par biais du logo CIM Internet).

- La Clause de non-responsabilité et la Politique de respect de la vie privée ou la Politique de respect de la vie privée doivent inclure dans la liste des partenaires le CIM et Gemius comme coresponsables de l'étude CIM Internet, avec le lien vers la page où se trouve la Politique de respect de la vie privée de Gemius.

Plusieurs de ces exigences sont reprises plus en détail dans le règlement de l'étude CIM Internet.

7. Références et sources

L'APD belge

[Page d'accueil citoyen | Autorité de protection des données \(autoriteprotectiondonnees.be\)](https://autoriteprotectiondonnees.be/)

Le Transparency & Consent Framework de l'IAB Europe

[TCF – Transparency & Consent Framework - IAB Europe](https://www.iab.com/privacy-center/transparent-consent/)

La liste de l'IAB Europe des CMPs et partenaires enregistrés

[CMP List - IAB Europe](https://www.iab.com/privacy-center/transparent-consent/cmp-list/)

[Vendors List - IAB Europe](https://www.iab.com/privacy-center/transparent-consent/vendors-list/)

L'APD belge et l'IAB Europe à propos de l'utilisation des advertising trackers

[IAB Europe's ad tracking consent framework found to fail GDPR standard | TechCrunch](https://www.techcrunch.com/2018/05/02/iab-europe-ad-tracking-consent-framework-found-to-fail-gdpr-standard/)

[IAB Europe comments on Belgian DPA report - IAB Europe](https://www.iab.com/privacy-center/transparent-consent/belgian-dpa-report/)

Des observations sur les plateformes de gestion du consentement

[Consent Management Platforms: The Definitive Guide for 2020 | Kevel \(Previously Adzerk\)](https://www.kevel.com/consent-management-platforms-the-definitive-guide-for-2020/)

Conseil en matière de classification des cookies

[Who we are and why we do it. Our story - Builtvisible](https://www.builtvisible.com/who-we-are-and-why-we-do-it-our-story/)

Un guide pour les entreprises

[TheGDPR-AGuideforBusinesses1.pdf \(algoodbody.com\)](https://www.algoodbody.com/the-gdpr-a-guide-for-businesses1.pdf)