Prénom:

Nom:

Pays:

Adresse:

Email:

Date de naissance:

Formulaire d'introduction d'une requête/plainte

Utilisez le présent formulaire si vous souhaitez introduire une requête/plainte auprès de l'Autorité de protection des données. Nous mettrons tout en œuvre pour vous répondre dans les meilleurs délais. L'Autorité de protection des données traitera toujours une requête ou une plainte d'abord comme une demande de médiation. Si aucun accord à l'amiable ne peut être trouvé, la demande de médiation initiale prendra la forme d'une plainte qui peut ensuite être transmise par le service de première ligne à la chambre contentieuse en vue d'un traitement sur le fond.

***Information au sujet du traitement des données à caractère personnel***

L’Autorité de protection des données traite vos données à caractère personnel car la loi l’y oblige en vue du traitement des plaintes et des requêtes. Nous traitons vos données à caractère personnel uniquement à des fins de gestion interne, à savoir le traitement rapide de votre réaction ou de votre demande d'information. Nous n'utilisons pas vos données à des fins commerciales et nous ne les transférons pas à des tiers.

Les données à caractère personnel sont conservées tant que cela est nécessaire dans le cadre de la formulation d’avis, de la sanction et du contrôle, et ce jusqu'à 10 ans après la clôture du dossier (en cas d'action en justice, jusqu'à la fin de la procédure). Dans le cadre de la coopération avec d’autres autorités européennes de protection des données, des informations du présent formulaire peuvent être partagées avec ces autorités.

L'identité du requérant/plaignant est en principe communiquée aux autres parties concernées.

Pour de plus amples informations concernant ce traitement de données à caractère personnel ou pour exercer vos droits d'accès, de rectification, de suppression de vos données et votre droit à la limitation du traitement, envoyez un e-mail à l'adresse dpo@apd-gba.be ou un courrier à l'Autorité de protection des données – DPO, rue de la Presse 35, 1000 Bruxelles.

## *Coordonnées*

**Nom\* :**

**Prénom\* :**

**Adresse\*** Rue\* : Numéro\* :

Code postal\* : Commune\* :

**Pays : Belgique**

**Téléphone :**

**E-mail\* :**

## *Votre requête/plainte\**

1. XXX souhaite faire part de ses inquiétudes auprès de l’Autorité de Protection des Données (APD) au sujet du secteur de la publicité comportementale (le « secteur »).
2. L’objectif de cette plainte est de demander une intervention de l’APD en vue de protéger les personnes concernées face aux violations à grande échelle et systématiques du régime de protection des données à caractère personnel perpétrées par Google et d’autres entreprises du secteur de la publicité comportementale. Cette plainte est soutenue par le rapport annexe de Dr. Johnny Ryan (“**the Ryan Report**”, le rapport Ryan).
3. La « publicité comportementale en ligne » (aussi dénomée “publicité programmatique”) est fondée sur deux systèmes principaux, les deux fonctionnant sur une technologie connue sous le nom de “real time bidding” (RTB), que l’on peut traduire par « offres en temps réel » :
* **« OpenRTB »** - utilisé virtuellement par toutes les grandes entreprises du secteur de la publicité et des médias.
* **«****Authorized Buyers »**, le système RTB exclusif de Google, anciennement appelé « DoubleClick Ad Exchange » (ou « AdX ») et récemment renommé « Authorized Buyers » (acheteurs autorisés).
1. Les deux systèmes permettent de produire des publicités personnalisées et ciblées sur les sites internet. Comme cela est souligné dans le rapport Ryan, « *à chaque fois qu’une personne charge une page sur un site web qui utilise la publicité programmatique, ses données personnelles sont transmises à des dizaines (voire centaines) d’entreprises*».
2. Selon le rapport Ryan, les données transmises comprennent:
* Ce que vous lisez ou regardez;
* Votre emplacement (OpenRTB inclut également une adresse IP complète);
* Description de votre appareil;
* Des identifiants de suivi uniques ou une « correspondance de cookies » pour permettre aux sociétés de technologie publicitaire d’essayer de vous identifier la prochaine fois que vous êtes vu, de sorte qu'un profil à long terme puisse être construit ou consolidé avec des données hors ligne vous concernant;
* Votre adresse IP (selon la version du système « RTB »);
* ID de segment du courtier de données, si disponible. Cela pourrait indiquer des facteurs comme votre tranche de revenus, votre âge et votre revenu;
* genre, habitudes, influence des médias sociaux, appartenance ethnique, orientation sexuelle, religion, tendance politique, etc. (selon la version du système “RTB”).
1. On dénombre trois sources significatives de préoccupations, liées à cette technologie.
	1. **Premièrement**, le secteur, qui au départ visait à aider les entreprises à produire des publicités personnalisées, a généré un mécanisme de transmission de masse de données personnelles.

Ce dernier :

* 1. collecte une grande quantité d’informations relatives aux personnes concernées qui dépasse la quantité d’informations nécessaires en vue de produire des annonces pertinentes et
	2. transmet ces informations à une foule de tierces parties, pour un éventail très large de finalités allant au-delà des objectifs qu’une personne concernée peut concevoir, et pour lesquels elle pourrait vouloir retirer son consentement ou s’opposer.

De telles opérations de profilage et de traitement de données à caractère personnel aussi intrusives et systématiques, ayant lieu au nom du profit, ne reposent sur aucun fondement juridique.

* 1. **Deuxièmement**, le mécanisme ne permet pas au secteur de contrôler la diffusion des données personnelles une fois qu’elles ont été transmises (voire même avant). Au vu du nombre impressionnant de destinataires recevant ces données, les responsables qui transmettent ces dernières ne peuvent pas protéger les individus du traitement ultérieur de leurs données, ni informer de manière effective les personnes concernées concernant les destinataires de ces données. Une fois transmises, les données personnelles ne sont tout simplement pas sécurisées et les carences de garanties organisationnelles mises en place démontrent que les violations de données personnelles en découlant sont propres à l’architecture de ce secteur et à la manière dont le traitement RTB est conçu. Ce traitement inéquitable des données, pour lequel des garanties suffisantes ne sont pas mises en oeuvre, n’est pas conforme aux réglementations en matière de protection des données à caractère personnel.
	2. **Troisièmement,** les données traitées comprennent souvent des données appartenant aux « catégories particulières de données à caractère personnel ». Les sites internet que les individus visitent peuvent contenir des indicateurs renseignant sur leur sexualité, origine ethnique, opinions politiques, etc. De tels indicateurs peuvent être explicites, ou déduits si efficacement, facilement et avec un niveau de précision si élevé (grâce aux techniques analytiques modernes), qu’ils permettent effectivement de révéler des données “sensibles”[[1]](#footnote-1). La vitesse à laquelle fonctionne le RTB signifie que les **données appartenant aux catégories particulières de données** peuvent être diffusées sans aucun consentement explicite ou sans qu’aucun contrôle sur cette transmission de données ne soit effectué. Ces données risquant d’être transmises à de nombreuses organisations qui pourraient les fusionner avec d’autres données, des profils d’individus extrêmement complexes peuvent alors être produits sans que la personne concernée ne le sache, et *a fortiori* sans son consentement. Le secteur facilite cette pratique et n’établit pas de mesures de protection suffisantes en vue d’assurer l’intégrité de ces données personnelles (et des données appartenant aux catégories particulières). Il est peu probable que les particuliers sachent que leurs données personnelles ont été diffusées et transmises, à moins qu’ils soient en mesure, d’une manière ou d’une autre, d’exercer leur droit d’accès aux données personnelles auprès d’un très grand nombre d’entreprises. Ce problème est aggravé par le fait que ces entreprises sont inconnues pour la plupart et inaccessibles aux personnes concernées, puisque les responsables de traitement des données qui collectent les données au départ ne fournissent que rarement des informations sur les destinataires, ou sur des catégories de destinataires, et que ces derniers n’informent pas les personnes concernées de la réception de ces données, conformément à leurs obligations prévues par l’article 14 du RGPD. Par ailleurs, il n’est pas sûr que ces entreprises aient une expertise en matière de respect de ce type de requêtes d’exercice de droits. Sans la mise en place de mesures de la part des autorités de contrôle, il est impossible d’assurer le respect des réglementations en matière de protection des données personnelles à l’échelle du secteur de la publicité programmatique.
1. À la lumière de ces préoccupations, l’APD est invitée:
	1. à prendre en compte les observations détaillées présentées ci-dessous ainsi que le rapport Ryan en annexe, afin que le service de première ligne de l’APD puisse déclarer la présente plainte recevable conformément à l’article 60 de la loi du 3 décembre 2017 portant création de l’Autorité de protection des données[[2]](#footnote-2) (ci-après “loi du 3 décembre 2017”) et à transmettre celle-ci à la chambre contentieuse;
	2. à demander à la chambre contentieuse de l’APD de décider qu'une enquête approfondie par le service d'inspection est nécessaire sur les questions que nous soulevons concernant le secteur de la publicité comportementale. Il est essentiel que la nature systématique des violations, détaillées dans cette plainte, soit reconnue en vue de combattre celles-ci;
	3. à exercer ses prérogatives prévues par le Chapitre VII du Règlement général sur la protection des données (RGPD) afin de se coordonner avec d’autres autorités de protection des données dans le but de mener une enquête commune sur les pratiques du secteur. Comme indiqué ci-dessous, des plaintes similaires ont été déposées auprès des autorités en charge de la protection des données au sein d’autres États membres de l’UE.
	4. En outre, nous invitons la chambre contentieuse de l’APD à traiter le dossier sur le fond, conformément à l’article 95 de la loi du 3 décembre 2017, en vue de formuler des avertissements et des réprimandes, conformément à l’article 100 de ladite loi, et, au besoin, de prendre des mesures coercitives.

## *Exposé des faits*

Le contexte lié au secteur de la publicité programmatique est décrit dans le rapport joint en annexe (le rapport Ryan). Nous renvoyons l’APD à ce rapport pour une présentation détaillée de ce secteur, de son fonctionnement et des problèmes en matière de protection des données qui sont inhérents au système.

Le secteur dispose d’une association commerciale, laquelle établit les paramètres et modèles d’utilisation. Il s’agit de l'Interactive Advertising Bureau (IAB), dont la branche européenne, IAB Europe, a mis en œuvre une politique et procédure sur les normes du secteur spécifique à l’Europe. En outre, en raison de la suprématie de Google sur le marché, Authorized Buyers dispose également de ses propres procédures et politiques.

* 1. *IAB Europe*
1. IAB Europe a créé un « Cadre européen de transparence et de consentement » (le Cadre[[3]](#footnote-3)). Ce dernier est fondé sur l’idée suivante : recueillir une seule fois le consentement de la personne concernée pour le partage ultérieur de ses données avec des tierces parties au cours du processus RTB.
2. On constate une faille fondamentale inhérente à la conception du système. Le Cadre reconnaît expressément qu’une fois que les données personnelles d’un individu sont diffusées, le responsable de traitement initial ainsi que la personne concernée par les données (par extension) perdent tout contrôle sur la façon dont les données sont utilisées. En effet, même lorsqu’un destinataire de données agit en violation de la loi, le Cadre autorise le responsable du traitement initial à continuer de transmettre des données au dit destinataire[[4]](#footnote-4). Dans ce cas, la personne concernée perd tout moyen lui permettant de déterminer la façon dont ses données sont ensuite utilisées.
3. Les données peuvent ensuite être transmises à un vaste écosystème de courtiers de données à caractère personnel (ou *data brokers*) et d’annonceurs. Ces tierces parties peuvent par la suite utiliser ces données comme bon leur semble, sans que la personne concernée n’ait son mot à dire, sans qu’elle n’en ait même connaissance et sans qu’elle puisse avoir de contrôle sur cette utilisation subséquente. Ces données peuvent être traitées pour de très nombreuses finalités : elles peuvent être fusionnées avec d’autres données ou encore être utilisées pour profiler la personne concernée, et ce à de nombreuses fins. Les utilisations finales de ces données peuvent ne pas avoir été mentionnées par le responsable du traitement au moment de son interaction avec la personne concernée. De telles utilisations finales des données pourraient être déstabilisantes pour les personnes concernées, si celles-ci venaient à en avoir connaissance[[5]](#footnote-5). De plus, il parait presque impossible pour le responsable de traitement initial d’informer les personnes concernées de toutes les utilisations finales car il n’a plus le contrôle sur les données une fois celles-ci transmises. Ce problème est inhérent au secteur et à la façon dont il est conçu.
4. En outre, et comme exposé dans le rapport Ryan, les données qui sont traitées peuvent inclure des données appartenant aux catégories particulières de données. Le fait que de telles données sensibles soient transmises sans le moindre contrôle ultérieur constitue donc une grande source de préoccupation.
5. Afin de préciser notre préoccupation concernant le Cadre, notons que ce dernier est conçu pour diluer la responsabilité sur les données traitées. Le Cadre anticipe le fait que des responsables de traitements qui transmettent des données personnelles pourraient les transmettre à des tierces parties sans base légale adéquate:

« *Un Vendeur peut décider, pour quelque raison que ce soit, de ne pas transmettre les données à un autre Vendeur, mais un Vendeur ne peut pas transmettre les données à autre Vendeur sans qu’il ne soit dûment justifié qu’il se fie au fait que le traitement des données personnelles de cet autre Vendeur repose sur une base juridique »*[[6]](#footnote-6)*.*

*« Si un Vendeur a obtenu ou obtient des données personnelles sans que l’accès à ces données et leur traitement ne repose sur une base juridique, le Vendeur doit rapidement cesser la collecte et le stockage de ces données et s’abstenir de les transmettre à d’autres parties, même si ces parties disposent d’une base juridique* »[[7]](#footnote-7).

1. Par conséquent, les responsables qui transmettent les données personnelles se voient conférer une marge d’appréciation pour décider s’il « *est dûment justifié que le traitement des données personnelles de cet autre Vendeur repose sur une base juridique ».* Dès lors, le cadre axé autour du consentement de la personne concernée peut être contourné. Un Vendeur peut interpréter librement ce qui est « dûment justifié » pour décider que la transmission des données personnelles à une tierce partie repose sur une base légale, potentiellement même lorsqu’un individu a expressément refusé de donner son consentement. L’intégralité du système repose par conséquent sur l’appréciation et le jugement du Vendeur et s’appuie sur des termes vagues et des paramètres mal définis, plutôt que sur l’information et le consentement de la personne concernée.
2. En résumé, le Cadre confère un pouvoir discrétionnaire au Vendeur, plutôt que de prendre en considération la position de la personne concernée. Cela vise à utiliser la base légale du consentement dans un contexte où les auteurs du Cadre sont conscients du fait que ce consentement sera difficile à obtenir pour toutes les étapes du traitement. Malheureusement, ce raisonnement ne prend que très peu en compte les droits à la protection des données personnelles des individus.
3. Notons que IAB Europe a récemment publié un communiqué de presse, suggérant une réforme du Cadre. Toutefois, ces propositions ne sont pas identifiées et les détails exposés dans le communiqué ne répondent pas suffisamment aux inquiétudes soulevées plus haut. De ce fait, nous pensons que ce communiqué de presse est l’occasion propice pour l’APD de mener une enquête sur tout le secteur, afin d’assurer des pratiques cohérentes et conformes aux réglementations en matière de protection des données.
	1. Authorized Buyers (acheteurs autorisés)
4. Authorized Buyers dispose d’une « Ligne de conduite »[[8]](#footnote-8) et de conditions commerciales d’utilisation. Cette “ligne de conduite” suscite de nombreuses préoccupations.
5. La Ligne de conduite fait passer la responsabilité en matière de protection des données des mains des responsables de traitement aux mains des tierces parties qui reçoivent les données. Par exemple la Ligne de conduite prévoit que (sic):

***“Restrictions en matière de données des appels d’offre RTB***

*L’acheteur peut stocker des cookies d’identification cryptés et un numéro d’indentification de publicité sur mobile dans le but d’évaluer les impressions et enchères à partir des données utilisateur obtenues antérieurement par l’acheteur. Toutes les autres données de l’appel d’offre (*callout data*), à l’exception des données de localisation, peuvent être conservées par l’acheteur après avoir répondu à un appel de publicité dans le seul but de prévoir la disponibilité de l’inventaire à travers le programme Authorized Buyers.*

*L’Acheteur n’est autorisé à conserver les données de l’appel d’offre que pendant la période de temps nécessaire à atteindre les objectifs mentionnés plus haut, et dans tous les cas, pour une durée ne dépassant pas les 18 mois.*

*À moins que l’Acheteur ne remporte une impression donnée, ce dernier ne doit pas : (i) utiliser des données d’appel d’offre pour cette impression en vue de créer des listes d’utilisateurs et de produire des profils d’utilisateurs ; (ii) associer des données d’appel d’offre pour cette impression avec des données de tierces parties ; (iii) partager des données de grilles tarifaires, sous forme agrégée ou non, avec des tierces parties, et ce d’aucune façon que ce soit”*[[9]](#footnote-9)*.*

***“Protection des données***

*Si l’Acheteur utilise, traite ou accède aux données personnelles rendues accessibles par Google qui permettent d’identifier directement ou indirectement un individu et qui proviennent de l’Espace économique européen (les « informations personnelles »), alors l’Acheteur doit :*

* *respecter toutes les lois, directives et réglementations en matière de protection des données de toute juridiction compétente ;*
* *utiliser ces informations personnelles et y accéder uniquement à des fins compatibles avec le consentement obtenu auprès de l’individu concerné par ces données personnelles :*
* *mettre en place des mesures organisationnelles techniques appropriées en vue de protéger les informations personnelles contre une perte, une mauvaise utilisation, un accès non autorisé et illégal, leur divulgation, déformation ou destruction, et*
* *garantir le même niveau de protection tel que celui exigé par les principes du Bouclier de Protection des Données UE – États – Unis (« Privacy Shield »).*

*L’acheteur vérifiera régulièrement que vous respectez cette obligation et avertira immédiatement Google, par écrit, si l’Acheteur n’est plus en mesure de respecter (ou s’il existe un risque réel que l’Acheteur ne soit plus en mesure de respecter) cette obligation, et le cas échéant, l’Acheteur cessera de traiter les informations personnelles ou prendra immédiatement d’autres mesures raisonnables et appropriées en vue de remédier à son incapacité de garantir un niveau suffisant de protection”*[[10]](#footnote-10)*.*

1. Ce passage suggère qu’une fois que les données personnelles sont transférées à un Acheteur, Authorized Buyers n’a plus de contrôle effectif sur la manière dont les données sont utilisées. Au contraire, il est admis que la tierce partie (l’Acheteur) puisse utiliser librement les données. Les seules restrictions imposées sont contractuelles et nous ne savons pas clairement dans quelle mesure ces dernières sont ou pourraient être appliquées. C’est aussi valable pour les « Conditions de protection des données Google Ads applicables aux Co-Responsables du Traitement »[[11]](#footnote-11).
2. En outre, même les restrictions qui sont imposées aux Acheteurs contiennent des limites inacceptables. Par exemple, dans la Ligne de conduite, on ne sait pas clairement quelles sont les restrictions imposées à un Acheteur dont l’offre a été retenue, les restrictions n’étant imposées qu’à ceux dont l’offre n’a pas été retenue («*à moins qu’un Acheteur ne remporte une impression, il ne doit pas…*»). L’absence évidente de contrôle donne lieu à de sérieuses préoccupations concernant la sécurité technique et organisationnelle des données concernées.
3. De plus, l’efficacité de la politique de protection des données personnelles dépend uniquement de la bonne volonté des tierces parties de respecter ou non les conditions de Authorized Buyers. Par conséquent, les garanties techniques permettant de protéger les données personnelles nous paraissent clairement insuffisantes.
4. **Moyens en droit**
5. Le contexte présenté ci-avant démontre que le traitement des données par Google et le secteur donne lieu à un risque important de violations du RGPD et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[[12]](#footnote-12) (ci-après “loi du 30 juillet 2018”).
6. Nous estimons que plusieurs des principes en matière de protection des données énoncés à l’article 5 du RGPD sont violés par Google et le secteur. Cependant, à ce stade et dans l’attente de la recevabilité de cette plainte par l’APD, nous n’exposons pas de manière exhaustive ces violations. Nous estimons que l’attention doit être portée en priorité sur la légalité des politiques présentées ci-avant (le “Cadre” d’IAB Europe et la “Ligne de conduite” de Google), plutôt que sur des cas particuliers de violations. Nous résumons nos principales préoccupations ci-dessous.
	1. *Intégrité et confidentialité*
7. Notre principale préoccupation est la suivante : les cadres et politiques actuels du secteur ne prévoient pas de protection suffisante contre la divulgation et le traitement non autorisés et potentiellement illimités des données personnelles.
8. L’article 5(1)(f) du RGPD exige que les données soient *« traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ».*
9. Le Cadre de IAB Europe, ainsi que la Ligne de conduite de Google, ne garantissent pas « une intégrité et confidentialité » appropriée des données personnelles, principalement pour les raisons suivantes :
10. Ils n’imposent pas aux responsables du traitement d’informer les personnes concernées au sujet des finalités auxquelles sont destinées leurs données à caractère personnel, ni des destinataires ou des catégories de destinataires auxquels ces données sont transmises;
11. Ils n’offrent pas aux personnes concernées l’opportunité de présenter leur point de vue aux vendeurs/destinataires des données au sujet de la manière dont leurs données personnelles peuvent être utilisées à des fins de profilage;
12. Ils n’accordent pas de droit formel aux personnes concernées de retirer leur consentement ou de s’opposer à l’utilisation de leurs données par les reponsables de traitements et les destinataires;
13. Ils ne mettent en place aucune mesure technique ou organisationnelle appropriée pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée visant à prévenir une utilisation ultérieure illégale et/ou non-autorisée.
	1. *Légalité et loyauté du traitement des données*
14. L’article 5(1)(a) du RGPD exige que les données à caractère personnel soient traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence).
15. L’article 6 fixe les conditions dans lesquelles un traitement des données à caractère personnel peut être réalisé de façon licite. En vertu de l’article 6(1), deux fondements de licéité peuvent potentiellement s’appliquer au secteur:
	1. la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
	2. le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.
16. Le consentement constitue le premier fondement de licéité énuméré par l’article 6 du RGPD et est considéré par le Cadre d’IAB Europe comme étant le fondement de licéité applicable au traitement de données du secteur visé dans la présente plainte. Pourtant, le secteur est intrinsèquement incapable d’obtenir un consentement approprié au sens de l’article 7 du RGPD. Cela est manifeste compte tenu du fait que les intermédiaires ne peuvent avoir de contact direct avec les personnes concernées.
17. Se baser sur les intérêts légitimes pour diffuser en grande quantité des appels d’offres RTB nous semble inapproprié. En effet, un intérêt légitime n’est pas absolu et devrait être mis en balance avec “les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel”. En particulier, il n’est pas équitable de justifier la transmission des données à caractère personnel à un très grand nombre d’entreprises sans la mise en place de mesures de sécurité appropriées si l’on prend en considération l’impact de cette transmission sur les droits et libertés des personnes concernées.
18. En outre, en vertu de l’article 9 du RGPD, le traitement des « *catégories particulières de données*» exige le consentement explicite si ces données n’ont pas été « *manifestement rendues publiques*» par la personne concernée et qu’aucune autre exception n’est applicable. Cependant, le Cadre de IAB Europe et la Ligne de conduite de Authorized Buyers autorisent le secteur à traiter les données personnelles sans consentement, dont des données réelles ou données induites portant sur l’origine ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l’appartenance syndicale, la santé, l’orientation ou la vie sexuelle, les données génétiques ou biométriques traitées aux fins d'identifier une personne physique de manière unique. En l’absence de consentement explicite à un tel traitement des données, ces pratiques se font en violation de l’article 9 du RGPD.
19. De surcroît, un consentement explicite est exigé lorsqu’est prise une *“décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques concernant [la personne concernée] ou l'affectant de manière significative de façon similaire”*. Le Groupe Article 29 (ou G29) identifie des instances où la publicité comportementale, telle qu’elle est mise en place par le secteur, pourrait affecter les personnes concernées de manière significative au sens de l’article 22 du RGPD[[13]](#footnote-13). Selon le G29, *“un traitement qui pourrait avoir peu d’incidences sur les personnes en général peut en fait avoir un effet significatif à l’égard de certains groupes de la société, tels que les groupes minoritaires ou les adultes vulnérables. Par exemple, une personne dont il est connu qu’elle éprouve des difficultés financières ou qui est susceptible d’éprouver de telles difficultés, et qui est régulièrement ciblée par des publicités pour des prêts à taux d’intérêt élevé, peut s’inscrire à ces offres et s’endetter davantage”*[[14]](#footnote-14)*.*
20. Aussi peut-on craindre que le secteur de la publicité programmatique traite des données personnelles et catégories particulières de données sans consentement valide. En effet, le Cadre prévoit un système dans lequel les données peuvent être traitées et transmises sans le consentement d’une personne concernée. Cela n’est pas légal, et ce traitement de données ne peut d’aucune faonn ﷽﷽﷽﷽﷽﷽ne concerne consentement d's. causer du tort, pourrait es ou philosophiques, l¡apnrecueillir et conserver des le logçon être considéré comme « *loyal* » ou « *transparent* ».
	1. *Finalité, minimisation et limitation dans le temps*
21. Le traitement des données par le secteur visé dans le cadre de cette plainte ne respecte pas l’article 5(1)(b) du RGPD en vertu duquel les données doivent être *“collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités”*. Le nombre de destinataires des données et les risques d’utilisations ultérieures non compatibles par ces destinataires entraînent des risques élevés pour les personnes concernées. De surcroît, le principe de minimisation inscrit à l’article 5(1)(c) du RGPD semble lui-aussi être mis à mal au vu du nombre de données traitées (voir rapport Ryan en annexe).
22. L’article 5(1)(e) précise également que les données personnelles traitées soient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Or, la Ligne de conduite de Authorized Buyers prévoit (sans pouvoir le garantir, en raison du manque de contrôle) que les données personnelles soient conservées pendant une durée de 18 mois. Les données personnelles sont donc susceptibles d’être conservées pendant de longues périodes de temps, sans finalité appropriée et identifiable.
	1. *Protection dès la conception et protection par défaut*
23. La publicité comportementale dépend de la capacité de cibler les individus à travers l’utilisation d’identifiants numériques qui sont associés à des appareils électroniques (qui, de nos jours, concernent un seul et même individu), ou de lier des individus à des appareils et à des contextes. Pour les individus, les identifiants sont difficiles d’accès et sont difficiles à récupérer en vue de contacter les responsables de traitement de données qui détiennent leurs informations personnelles, ce qui génère un déséquilibre notoire et un obstacle considérable à l’exercice des droits liés à la protection de leur données personnelles, tels que les droits à l’accès, à l’effacement, à l’opposition, à la portabilité des données et à la limitation du traitement.
24. Cela accentue le problème plus large concernant le principe fondamental de **loyauté** énoncé dans l’article 5 du RGPD : les responsables de traitement accèdent facilement aux identifiants afin de cibler les individus, alors que ces mêmes individus ne sont pas véritablement en mesure d’utiliser ni de contrôler ces identifiants. Cela suscite des préoccupations, notamment au regard de l’article 25, portant sur la protection des données dès la conception et de la protection des données par défaut, qui impose notamment aux responsables de traitement l’obligation positive de mettre en œuvre les mesures techniques et organisationnelles appropriées pour *“assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée”* ainsi que pour garantir que *“par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée”*.
	1. *Analyse d'impact relative à la protection des données*
25. Au vu de l’étendue du traitement de données à caractère personnel, du traitement de données sensibles, du nombre très élevé de destinataires de données, de la création de profils comportementaux, de la surveillance systématique d’une zone accessible au public et du croisement d’ensembles de données, il est probable que le traitement des données du secteur est “susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques”. Dès lors, l’article 35 exige-t-il une analyse d'impact relative à la protection des données. Actuellement, à notre connaissance, aucune analyse d’impact n’a été menée, ou à tout le moins rendue publique.
26. **Quant à la compétence de l’Autorité de protection des données**
27. L’APD est compétente pour traiter cette plainte en raison des traitements de données à caractère personnel présentés dans le cadre de celle-ci et tels que décrits dans le rapport Ryan en annexe.
	1. *Traitement des données*
28. L’article 4 du RGPD indique que les « données à caractère personnel » constituent « *toute information se rapportant à une personne physique identifiée ou identifiable*». Ces données comprennent les « identifiants en ligne » quand ils permettent d’identifier directement ou indirectement un individu. La Cour européenne de justice a confirmé que les adresses IP peuvent constituer des données personnelles[[15]](#footnote-15). En outre, les données personnelles « pseudonymisées » sont également considérées comme étant des données personnelles.
29. Le traitement et la transmission des données personnelles des personnes concernées au cours du « processus RTB » implique le traitement de données à caractère personnel, telles que les adresses IP ou des données de localisation.
	1. *Juridiction*
30. XXX est domicilié-e en Belgique et est un-e utilisateur-rice des technologies de communication internet.
31. Conformément à l’article 3, §2 du RGPD : “Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.”

1. Dès lors, in casu, le RGPD s’applique dans la mesure où le secteur visé dans le cadre de la présente plainte traite des données à caractère personnel en vue de proposer des annonces à des personnes se trouvant au sein du territoire belge, et ce indépendamment des lieux d’établissement de ces entreprises
2. En vertu de l’article 51 du RGPD et des articles 4 et suivants de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, l’APD constitue l’autorité de contrôle de la Belgique.
3. Les devoirs de l’APD sont énoncés à l’article 57 du RGPD et comprennent des devoirs généraux, tels que le contrôle de l’application et du respect du RGPD mais aussi, conformément à l’article 58, la possibilité de *« mener des enquêtes sous la forme d'audits sur la protection des données ».*
4. L’APD a également pour mission de traiter les plantes introduites par des personnes concernées dans les conditions prévues par les articles 57 et suivants de la loi du 3 décembre 2017.
5. D’autres plaintes ont également été déposées auprès des autorités de la protection des données d’Irlande et du Royaume-Uni, et de nouvelles plaintes sont en cours de rédaction en vue d’être déposées auprès d’autorités de contrôle d’autres Etats membres de l’Union européenne. Compte tenu de la portée géographique des questions soulevées dans cette plainte et du nombre d’entreprises concernées, il serait approprié que les nombreuses autorités de contrôle nationales examinent cette question à l’unisson. Aussi invitons-nous l’APD à prendre contact avec d’autres autorités de contrôle afin de mener une enquête commune, conformément à l’article 62 du RGPD.
6. **Requêtes**
7. La présente plainte est adressée à l’Autorité de protection des données. Nous appelons l’APD à prendre les mesures suivantes dans la limite des pouvoirs et mandat qui lui sont conférés.
8. *Traitement de la plainte:*
9. Tout d’abord, nous invitions l’APD:
	1. à prendre en compte les observations détaillées présentées dans cette plainte ainsi que le rapport Ryan en annexe, afin que le service de première ligne de l’APD puisse déclarer la présente plainte recevable conformément à l’article 60 de la loi du 3 décembre portant création de l’Autorité de protection des données et à transmettre celle-ci à la chambre contentieuse;
	2. à demander à la chambre contentieuse de l’APD de décider qu'une enquête approfondie par le service d'inspection est nécessaire sur les questions que nous soulevons concernant le secteur de la publicité comportementale. Il est essentiel que la nature systématique des violations, détaillées dans cette plainte, soit reconnue en vue de combattre celles-ci;
	3. à exercer ses pouvoirs prévus par le Chapitre VII du Règlement général sur la protection des données afin de se coordonner avec d’autres autorités de protection des données dans le but de mener une enquête commune sur les pratiques du secteur. Comme déjà indiqué, des plaintes similaires ont été déposées auprès des autorités en charge de la protection des données au sein d’autres États membres de l’UE.
	4. En outre, nous invitons la chambre contentieuse de l’APD à traiter le dossier sur le fond conformément à l’article 95 de la loi du 3 décembre 2017 en vue de formuler des avertissements et des réprimandes conformément à l’article 100 de ladite loi, et, au besoin, de prendre des mesures coercitives.
10. *Enquête par le service d’inspection*
11. En vertu de l’article 72 de la loi du 3 décembre 2017, l’APD est habilitée à enquêter sur le secteur visé par la présente plainte (cela correspond aux enquêtes sous forme d’audit prévus à l’article 58(1)(b) du RGPD). Cela signifie que l’ *« l'inspecteur général et les inspecteurs peuvent procéder à toute enquête, tout contrôle et toute audition, ainsi que recueillir toute information qu'ils estiment utile afin de s'assurer que les principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la présente loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel, sont effectivement respectées. »* Spécifiquement, nous souhaiterions que l’APD enquête sur les éléments suivants:
	1. L’absence de garanties nécessaires à l’intégrité et à la confidentialité des données personnelles traitées via openRTB et Authorized Buyers;
	2. L’inadéquation de la base de licéité des traitements RTB sur laquelle se fonde le “Cadre” d’IAB Europe et la “Ligne de conduite” de Google pour légitimer les traitements de publicité comportementale;
	3. L’absence de consentement explicite pouvant servir d’exception à l’interdiction de traiter des catégories particulières de données;
	4. L’évaluation de l’analyse d’impact relative à la protection des données, si celle-ci existe, concernant l’utilisation de openRTB et Authorized Buyers par le secteur ayant recours à la publicité programmatique.
12. Nous invitions l’APD à exercer ses pouvoirs en vertu de la sous-section 2 du Chapitre IV de la loi du 3 décembre 2017 vis-à-vis d’IAB Europe et Authorized Buyers de Google. Compte tenu de l’impossibilité pour les personnes concernées, en tant que particuliers, d’évaluer et de s’assurer du respect des obligations du secteur, en raison de l’échelle et de la complexité de ces opérations, l’APD est le seul opérateur à même de mener à bien cette évaluation.
13. **Prochaines étapes**
14. Pour les raisons établies plus haut, nous demandons à l’APD d’ouvrir une enquête sur les activités du secteur de la publicité programmatique et de prendre les mesures décrites dans cette plainte.
15. De plus, compte tenu de la portée et de la complexité des activités décrites ci-dessus, toute personne peut être affectée, et ce à tout moment, ce qui représente un problème majeur. Ces activités affectent les individus, dont des personnes vulnérables, de toutes les couches de la société et à travers toute l’Europe. Aussi invitons-nous l’APD à entrer en contact avec ses homologues des autres pays membres de l’UE afin de mener une enquête commune, conformément à l’article 62 du RGPD.

Nous nous réservons le droit, le cas échant, de compléter cette plainte avec autant d’autres éléments de preuve et arguments que nécessaires.

Dans l’attente, nous restons à votre disposition en cas de besoin. Par ailleurs, nous vous serions très reconnaissants de nous tenir informés des mesures prises en réponse à notre requête et ce conformément à l’article 77(2) du RGPD.

## *Identification du traitement concret, en mentionnant si possible les coordonnées du responsable du traitement/sous-traitant*

 Le traitement concret est décrit dans le rapport Ryan en annexe.

Nous identifions trois (catégories de) « responsables » :

* IAB Europe, dont l’adresse est Rond-point Robert Schuman 11, 1000 Bruxelles, Belgique ;
* GOOGLE IRELAND LIMITED, dont le siège social est établi à 4 Barrow Street, Dublin, Irlande ;
* Les responsables de traitements du secteur de la publicité programmatique (situés en Europe ou ailleurs) utilisant les mécanismes openRTB et Authorized Buyers pour cibler des personnes concernées situées en Belgique.

## *Date et signature*

**Annexe: Le rapport Ryan**

**Rapport du Dr Johnny Ryan – La publicité comportementale et les données personnelles**

*Traduction d’un extrait du rapport complet, disponible ici via ce lien:*
<https://brave.com/Behavioural-advertising-and-personal-data.pdf>

**Comment les données personnelles sont utilisées dans la publicité comportementale en ligne**

Chaque fois qu’une publicité comportementale ciblée est diffusée à une personne visitant un site internet, le système qui sélectionne la publicité à montrer à cette personne transmet les données personnelles de cette dernière à des centaines, voire des milliers d’entreprises.

Ce système est connu sous le nom de « Real-Time biding » (enchères en temps réel). On parle aussi de « publicité programmatique » (ce qui veut tout simplement dire qu’il s’agit d’un système automatique).

Les données personnelles partagées comprennent l’URL de chaque page visitée par un internaute, son adresse IP (à partir de laquelle la localisation géographique peut être déduite), des détails concernant son appareil et plusieurs identifiants uniques sur l’internaute qui ont pu être conservés auparavant, tout cela dans le but de construire un profil de long-terme sur cette personne.

Au cours de la période de grâce qui a vu la création du RGPD, le secteur de la publicité en ligne a mis en place des mesures de contrôle non appropriées et non suffisantes en vue de faire respecter les réglementations en matière de protection des données personnelles par les nombreuses entreprises qui reçoivent ces données.

**Comment les données personnelles sont « transmises »**

Une part importante des médias en ligne et des entreprises du secteur de la publicité en ligne utilisent un système dénommé « **RTB** » : le « real time bidding ». Il existe deux versions de ce système.

* **« OpenRTP »,** qui est utilisé par les plus grandes entreprises du secteur des médias et de la publicité en ligne.
* **« Authorized Buyers »,** le système exclusif de Google, anciennement « DoublClik Ad Exchange » (connu sous le nom de « AdX »).

Google utilise à la fois OpenRTB mais aussi son propre système, « Authorized Buyers ».

Pour ces deux versions du RTB, des cahiers des charges sont accessibles au public. Les documents en question révèlent que, à chaque fois qu’une personne charge une page sur un site internet qui intègre des publicités via la technologie RTB, ses données personnelles sont transmises à des dizaines, voire des centaines d’entreprises. Voici quelques exemples de données qui sont partagées :

* Ce que vous lisez ou regardez
* Votre localisation (OpenRTB inclut aussi l’adresse IP complète).
* Une description de votre appareil
* Les numéros d’identification uniques de traçabilité ou « cookie match », qui permettent aux entreprises des technologies publicitaires de vous identifier la prochaine fois que vous serez repéré, le but étant d’établir ou consolider un profil sur le long terme avec des données personnelles hors ligne vous concernant.
* Votre adresse IP (en fonction de la version du « système RTB » utilisé).
* Les « segment ID » d’un courtier en données, si ces derniers sont accessibles. Cela peut renseigner sur votre tranche de revenus, votre âge, votre genre, vos habitudes, votre influence sur les réseaux sociaux, votre origine ethnique, votre religion, vos orientations politiques, etc. (en fonction de la version du « système RTB » utilisé).

Un résumé plus complexe des données personnelles comprises dans les appels d’offres RTB est présenté dans le rapport original en anglais, dans l’Annexe 1. et 2. Des extraits pertinents des cahiers des charges sont présentés dans les annexes 1 et 4.

**Comment cela fonctionne.**

Un schéma du flux d’information est présenté ci-dessous :



La transmission des données personnelles via la technologie RTB est communément reconnue sous le nom d’ « appel d’offre RTB ». Les données sont généralement largement partagées, l’objectif étant de lancer un appel d’offre à des entreprises susceptibles de vouloir montrer une publicité à une personne qui vient de charger la page. Un appel d’offre RTB est transmis au nom des sites internet par des entreprises désignées comme des « supply side platforms » (SSPs), des plateformes automatisées destinées aux éditeurs ou à toute personne louant des espaces publicitaires, et par des « Ad exchanges » afin de « multiplier » les « demand side partners » (DSPs), des plateformes qui permettent à un annonceur / un marketeur de cibler ses campagnes et de centraliser ses opérations d’achats publicitaires, qui décident ensuite de déposer ou non une offre pour cibler la personne en question avec une publicité.

La RTB n’établit aucun contrôle concernant le « devenir » des données personnelles une fois qu’un SSP ou qu’un Ad Exchange transmet les donnés d’un appel d’offre RTB. Même si la transmission de ces données est sécurisée, aucune mesure technique n’est instaurée en vue de prévenir le destinataire d’associer ces données avec d’autres données afin de créer une base de données personnelles avec des partenaires commerciaux, ou de les revendre. Une fois que les DSPs reçoivent les données personnelles, ces derniers peuvent les vendre en toute liberté à des partenaires commerciaux, et ce, comme bon leur semble.

C’est particulièrement inquiétant dans la mesure où ces données appartiennent sans doute aux « catégories particulières » de données personnelles, telles que définie dans le RGPD. Ces données permettent notamment de savoir ce qu’une personne concernée regarde sur le web et renseignent souvent sur la localisation spécifique de cette dernière. Ces données permettent d’identifier l’orientation sexuelle, les croyances religieuses, les orientations politiques ou encore l’origine ethnique. Ajoutons à cela les données de type « segment ID », qui permettent de savoir dans quelle catégorie de personne un courtier en données a « rangé » un individu.

En conclusion, ce système de publicité programmatique en ligne ne prévoit aucune protection des données personnelles. Il s’agit d’une pratique généralisée très préoccupante. L’envergure du secteur de la publicité comportementale affecte virtuellement les droits fondamentaux de chaque personne naviguant sur internet en Europe.

1. Voir « *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*» (wp251rev.01) : « le profilage peut créer des catégories particulières de données par déduction, à partir de données qui ne font pas partie des catégories particulières de données à proprement parler mais qui le deviennent lorsqu’elles sont associées à d’autres données. Par exemple, il est possible de déduire des données relatives à l’état de santé d’une personne en analysant des données liées à ses courses alimentaires associées à des données relatives à la qualité et propriétés énergétiques de ces aliments ». Notons que (comme cela est confirmé dans l’Affaire Nowak de la CJUE) même les données déduites concernant un individu qui sont erronées restent tout de même des données à caractère personnel. Si cela n’était pas le cas, le « droit à la rectification » ne pourrait jamais être exercé/invoqué. [↑](#footnote-ref-1)
2. M.B. 10-01-2018. [↑](#footnote-ref-2)
3. <http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf> [↑](#footnote-ref-3)
4. Le Cadre prévoit que (traduction libre) « si un CMP pense raisonnablement qu’un Vendeur ne respecte pas le Cahier des charges, les Politiques ou la loi, il doit immédiatement porter plainte auprès du MO conformément aux procédures du MO et peut suspendre ses activités avec le Vendeur en attendant que le problème soit traité ». Le responsable du traitement des données jouit alors d’une marge de manœuvre démesurée et peut continuer à traiter et partager des données personnelles, même si ce responsable sait que le destinataire agit en violation des réglementations en matière de protection des données à caractère personnel. [↑](#footnote-ref-4)
5. Au paragraphe 20 du Rapport Ryan, il est indiqué clairement que la dorénavant célèbre Cambridge Analytica constitue l’un des exemples de destinataires des données personnelles. [↑](#footnote-ref-5)
6. Traduction libre. [↑](#footnote-ref-6)
7. Traduction libre. [↑](#footnote-ref-7)
8. <https://www.google.com/doubleclick/adxbuyer/guidelines.html> [↑](#footnote-ref-8)
9. Traduction libre: “RTB Callout Data Restriction. Buyer may store the encrypted cookie ID and mobile advertising identifier for the purpose of evaluating impressions and bids based on user-data previously obtained by the Buyer. All other callout data except for Location Data may be retained by Buyer after responding to an ad call for the sole purpose of forecasting the availability of inventory through the Authorized Buyers program. Buyer is permitted to retain callout data only for the length of time necessary to fulfill the relevant purposes stated above, and in any event, for no longer than 18 months. Unless Buyer wins a given impression, it must not: (i) use callout data for that impression to create user lists or profile users; (ii) associate callout data for that impression with third party data; or (iii) share rate card data in any form, including but not limited to aggregate form, with third parties”. [↑](#footnote-ref-9)
10. Traduction libre: “Data Protection. If Buyer accesses, uses, or processes personal information made available by Google that directly or indirectly identifies an individual and that originated in the European Economic Area (“Personal Information”), then Buyer will:

comply with all privacy, data security, and data protection laws, directives, regulations, and rules in any applicable jurisdiction;

use or access Personal Information only for purposes consistent with the consent obtained by the individual to whom the Personal Information relates;

implement appropriate organizational and technical measures to protect the Personal Information against loss, misuse, and unauthorized or unlawful access, disclosure, alteration and destruction; and

provide the same level of protection as is required by the EU-US Privacy Shield Principles.

Buyer will regularly monitor your compliance with this obligation and immediately notify Google in writing if Buyer can no longer meet (or if there is a significant risk that Buyer can no longer meet) this obligation, and in such cases Buyer will either cease processing Personal Information or immediately take other reasonable and appropriate steps to remedy the failure to provide an adequate level of protection”. [↑](#footnote-ref-10)
11. <https://privacy.google.com/businesses/controllerterms/> [↑](#footnote-ref-11)
12. M.B. 05-09-2018. [↑](#footnote-ref-12)
13. Voir G29, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251rev.01, p.24 : « Dans de nombreux cas typiques, la décision de présenter une publicité ciblée fondée sur le profilage, telle qu'une publicité pour un magasin de mode en ligne grand public, basée sur un simple profil démographique n'affectera pas les personnes concernées de façon similaire de manière significative : « les femmes de la région bruxelloise âgées de 25 à 35 ans qui sont susceptibles de s’intéresser à la mode et à certains articles d’habillement ». Toutefois, il se peut que ce soit le cas, selon les caractéristiques particulières de la situation, y compris en ce qui concerne:

• le caractère intrusif du processus de profilage, y compris le suivi des personnes sur différents sites web, appareils et services;

• les attentes et les souhaits des personnes concernées;

• la façon dont l’annonce est diffusée; ou

• le recours aux vulnérabilités connues des personnes concernées visées ». [↑](#footnote-ref-13)
14. Ibidem. [↑](#footnote-ref-14)
15. Case C-582/14 *Breyer.* [↑](#footnote-ref-15)