PLAINTE AU TITRE DE L'ARTICLE 77(1) DU RGPD

1. FAITS

1.1. Responsable du Traitement / Défendeur

Cette plainte est dirigée contre Google LLC („Google"), Amphitheatre Parkway, Mountain View, CA 94043, États Unis, en tant que fournisseur du système d'exploitation Android.

1.2. Personne concernée / Demandeur

[redacted]e

La personne concernée nous a mandatés (l'association noyb – Centre Européen pour les Droits Numériques) afin de la représenter conformément à l'article 80, paragraphe 1 du RGPD (Pièce 1).

1.3. Objet du consentement allégué (*À quoi la personne concernée a-t-elle prétendument consenti?*)

Le Responsable du Traitement utilise une politique de confidentialité (Pièce 2) ainsi que des conditions générales d'utilisation (Pièce 3) qui sont applicables à compter du 25 mai 2018 et auxquelles la personne concernée a dû consentir.

En acceptant les conditions d'utilisation, la personne concernée doit automatiquement accepter la politique de confidentialité également car les conditions d'utilisation incorporent la politique de confidentialité :

> *" Les Règles de confidentialité de Google expliquent comment nous traitons vos données à caractère personnel et protégeons votre vie privée lors de votre utilisation de nos Services. En utilisant nos Services, vous acceptez que Google puisse utiliser ces données conformément à ces Règles de confidentialité de Google."*

Traduction anglaise informelle:

COMPLAINT UNDER ARTICLE 77(1) GDPR

1. FACTUAL BACKGROUND

1.1. Controller / Respondent

This complaint is filed against Google LLC („Google"), Amphitheatre Parkway, Mountain View, CA 94043, USA, as the provider of the Android operating system.

1.2. Data subject / Complainant

[redacted]

The data subject has requested us (the non-profit noyb – European Center for Digital Rights) to represent him under Article 80(1) of the GDPR (attachment 1).

1.3. Subject of the alleged consent (*What did the data subject allegedly consent to?*)

The controller uses a privacy policy (attachment 2) and terms of service (attachment 3) that are applicable from May 25th 2018 onwards and that the data subject had to agree to.

By agreeing to the terms, the data subject automatically has to agree to the privacy policy too, as the terms include the privacy policy in the contract:

> *"Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies."*

Les politiques de confidentialité incluent également des catégories spéciales de données au titre de l'article 9(1) du RGPD car les données des smartphones comprennent inévitablement des informations sur les croyances politiques, philosophiques ou religieuses, sur l'orientation sexuelle, des données de santé etc.

Toutefois, les opérations de traitement que le Responsable du Traitement choisit de fonder sur chaque base juridique spécifique en vertu de l'article 6 et de l'article 9 du RGPD restent à déterminer.

Le Responsable du Traitement se contente d'énumérer quatre bases juridiques pour un traitement licite en vertu de l'article 6 du RGPD (consentement, intérêt légitime, traitement nécessaire pour l'exécution d'un contrat et obligations légales) dans sa politique de confidentialité sans indiquer exactement sur quelle base juridique le Responsable du Traitement se fonde pour chaque traitement spécifique.

Il est donc impossible de déterminer clairement quels traitements précis sont basés sur chaque base juridique spécifique en vertu des articles 6 et 9 du RGPD.

Certaines opérations de traitement pour lesquelles le Responsable du Traitement s'appuie explicitement sur le consentement :

- *« Nous ne communiquons vos informations personnelles à des tiers qu'avec votre consentement. »*
- *« Nous vous demanderons votre consentement explicite à partager des informations personnelles sensibles. »*

Dans chaque situation, le Responsable du Traitement a exigé de la personne concernée d'„accepter" l'ensemble de sa politique de confidentialité ainsi que ses conditions d'utilisation.

Cela conduit à notre hypothèse préliminaire, à savoir que tous les traitements décrits dans le présent document sont fondés sur le consentement ou que le Responsable du Traitement a tout du moins laissé la personne concernée croire que toutes ces opérations sont (également) fondées sur l'article 6(1)(a) et/ou sur l'article 9(2)(a) du RGPD.

The policies also include special categories of data under Article 9(1) of the GDPR, because phone data inevitably includes information about political, philosophical or religious beliefs, sexual orientation, health information etc.

It remains, nevertheless, unclear which exact processing operations the controller chooses to base on each specific legal basis under Article 6 and Article 9 of the GDPR.

The controller simply lists four bases for lawful processing under Article 6 of the GDPR (consent, legitimate interest, providing a contract and legal obligations) in his privacy policy without stating exactly the legal bases he relies upon for each specific processing operation.

It is therefore impossible to determine, which exact processing operations are based on each specific legal basis under Article 6 and Article 9 of the GDPR.

Some of the processing operations that the controller does explicitly base on consent are:

- *"We'll share personal information outside of Google when we have your consent."*
- *"We'll ask for your explicit consent to share any sensitive personal information."*

In any case, the controller required the data subject to "agree" to the entire privacy policy and to the terms.

This leads to our preliminary assumption, that all processing operations described therein are based on consent, or that the controller at least led the data subject to believe that all these processing operations are (also) based on Article 6(1)(a) and/or Article 9(2)(a) of the GDPR.

Cette politique de confidentialité n'est pas uniquement une „information", comme exigée, par exemple, au titre de l'article 14 du RGPD, car le Responsable du Traitement fournit non seulement cette information à l'utilisateur, mais oblige aussi l'utilisateur à „consentir" ou à „accepter" cette charte.

Comme indiqué ci-dessous (section 1.6 de la présente plainte), il devra être déterminé dans le cadre de cette procédure dans quelle mesure le Responsable du Traitement fonde les opérations de traitement sur les articles 6(1)(a) et 9(2)(a).

1.4. Acte de consentement *(Comment la personne concernée a-t-elle supposément consenti?)*

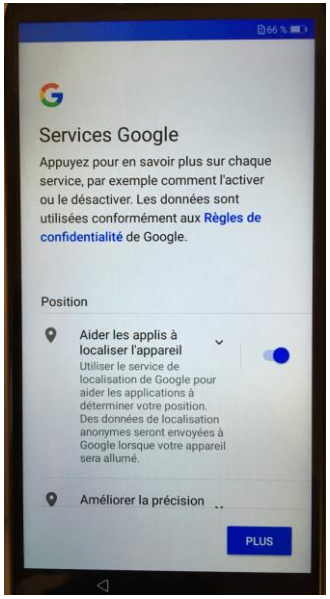
Lorsque la personne concernée a allumé son nouveau téléphone pour la première fois ("Huawei Y6 2018 noir"), elle a été contrainte d'accepter la politique de confidentialité et les conditions d'utilisation. Il n'y avait pas d'option pour utiliser le téléphone sans préalablement donner son consentement:

This privacy policy is clearly not only an "information", as required, for example, under Article 14 of GDPR, because the controller does not only provide this information to the user, but also forces the user to "consent" or "agree" to this policy.

As mentioned below (section 1.6 of this complaint), it will ultimately have to be determined in the course of this procedure, to what extent the controller bases processing operations on Article 6(1)(a) and 9(2)(a).

1.4. Act of consent (*How did the data subject allegedly consent?*)

When the data subject activated a new phone for the first time (a "Huawei Y6 2018 black") he was forced to "agree" to the privacy policy and the terms. There was no option to use the phone without consenting:



1.5. Nécessité d'enquêter au titre de l'article 58 du RGPD

Le Responsable du Traitement ne fournissant pas les informations requises par la loi sur les traitements d'informations en question, nous considérons qu'il est nécessaire que l'Autorité enquête sur l'objet spécifique du consentement allégué et sur la base juridique de tous les traitements effectués en vertu des pouvoirs qui lui sont conférés par l'article 58 du RGPD. Cela devrait inclure l'exigence de la liste des activités de traitement visées à l'article 30(4) du RGPD.

Nous croyons savoir que le Responsable du Traitement est tenu de divulguer tous les faits pertinents dans une réponse à cette plainte. Ce processus sera relativement simple car le Responsable du Traitement aurait dû documenter toutes les opérations de traitement et (nous l'espérons sincèrement) savoir sur quelle base juridique il cherche à s'appuyer.

1.6 Limitation de la plainte au traitement des données fondé sur l'article 6(1)(a) et/ou sur l'article 9(2)(a) du RGPD

Pour des raisons pratiques, la portée de la présente plainte est expressément limitée à toute opération de traitement fondée en tout ou en partie sur l'article 6(1)(a) et/ou sur l'article 9(2)(a) du RGPD. À notre connaissance, ces articles servent de base à toutes les opérations de traitement décrites dans la politique de confidentialité du Responsable du Traitement, mais cela dépendra du résultat de votre enquête.

Néanmoins, rien dans la présente plainte n'indique que d'autres bases juridiques sur lesquelles le Responsable du Traitement peut s'appuyer ne sont pas également invalides ou ne peuvent faire l'objet d'actions judiciaires ultérieures.

1.5. Need to investigate further details under Article 58 GDPR

As the controller does not provide the legally required information about the processing operations in question, we believe that it would be necessary for the supervisory authority to investigate the concrete subject of the alleged consent and the legal basis for all processing operation, under the powers vested on it by Article 58 of the GDPR. This should include requesting the record of processing activities, under Article 30(4) of the GDPR.

It is our understanding that the controller has an obligation to disclose all relevant facts in response to this complaint. This process will be rather straight-forward, as the controller should have documented all processing operations and (hopefully) knows which legal basis he seeks to rely on.

1.6 Limitation of complaint to processing based on Article 6(1)(a) and/or Article 9(2)(a)

For practical reasons, the scope of this complaint is explicitly limited to any processing operations that are wholly or partly based on Article 6(1)(a) and/or Article 9(2)(a) of the GDPR. Our current understanding is, that these are used as bases for all processing operations described in the controller's privacy policy, but this is subject to the outcome of your investigation.

Nevertheless, nothing in this complaint shall indicate that other legal bases the controller may rely on are not equally invalid or may not be equally the subject of subsequent legal actions.

2. DISCUSSION

2.1. Remarques préliminaires

Le consentement joue un rôle clé dans le traitement des données personnelles car il permet aux personnes concernées de contrôler si leurs données personnelles font l'objet d'opérations de traitement.

Consentement „libre"
L'élément «essentiel» du consentement est probablement le fait qu'il a été donné *librement*, tel que précisé à l'article 4(11) et spécifié à l'article 7(4) du RGPD. Dès lors, cette plainte porte principalement sur l'acte de consentement en l'espèce, lequel ne saurait être considéré comme un acte *«libre»*.

Comme les traitements dans le cadre de cette plainte sont déjà illégaux pour ce motif, nous invitons l'autorité de contrôle à ne pas enquêter sur d'autres questions si elle rejoint notre opinion concernant l'élément légal du consentement «*librement*» donné.

Par mesure de précaution procédurale, nous invoquons également un certain nombre d'autres motifs pour démontrer pourquoi le Responsable du Traitement ne peut guère invoquer le consentement allégué. Afin de rationaliser cette plainte, nous les avons résumés à la fin de celle-ci (voir section 2.3 de la présente plainte). Nous estimons en effet que cette plainte peut être tranchée sur le seul élément du consentement donné «*librement*».

Charge de la preuve
L'article 6(1) du RGPD impose une interdiction générale de tout traitement, à moins que le Responsable du Traitement puisse démontrer qu'il s'est conformé à l'une des exigences énoncées dans cet article. L'article 7(1) souligne en outre l'obligation spécifique de démontrer l'existence d'un consentement valide :

> *"Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant".*

La charge de la preuve de démontrer que le traitement est légal et que le consentement a été obtenu est donc confiée au Responsable du Traitement - et non à l'autorité de surveillance ou à la personne concernée.

2. LEGAL ANALYSIS

2.1. Introduction

Consent plays a central role in the processing of personal data, since its main purpose is to give data subjects control over whether or not personal data concerning them will be processed.

Focus on "freely" given consent
The 'core' element of consent is probably the fact that it must be *freely* given, as clarified in Article 4(11) of the GDPR and further specified in Article 7(4) of the GDPR. Thus, this complaint focuses primarily on the act of consent, which, in the present case, we do not see as "*free*".

As the processing operations within the scope of this complaint are already unlawful on this ground, we invite the supervisory authority not to investigate other issues, should it join our view in relation to the legal element of "*freely*" given consent.

As a matter of procedural precaution, we also rely on a number of other grounds to demonstrate why the controller cannot rely on the alleged consent. In order to streamline this complaint, we have consequently summarised them at the end of the complaint (see point 2.3 of this complaint), since we believe that this complaint can be decided on the element of "*freely*" given consent alone.

Burden of proof
Article 6(1) of the GDPR imposes a general prohibition of any processing operation, unless the controller can demonstrate that it complied with one of the requirements contained therein. Article 7(1) further highlights the specific obligation to demonstrate valid consent:

> "*[w]here processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data*".

The burden of proof to demonstrate that the processing operation is lawful and that valid consent was obtained is hence placed on the controller, not the Supervisory Authority or the data subject.

2.2. Consentement libre et éclairé

Le consentement ne peut être un motif légal de traitement que si les personnes concernées se voient offrir un choix réel et réaliste d'accepter ou de refuser les conditions d'un service ou de refuser ces conditions sans préjudice. Autrement dit, le consentement ne sera pas valide, si la personne concernée n'a pas de choix véritable ou réel, se sent obligée de consentir ou subira des conséquences négatives si elle ne consent pas, comme indiqué dans les lignes directrices du Groupe de Travail de l'Article 29 sur le consentement en vertu du Règlement 2016/679 (WP259) du 10 avril 2018.

Le Responsable du Traitement a procédé à un traitement illégal des données personnelles de la personne concernée en violation du RGPD. Ce traitement illicite est basé sur un consentement qui a été "forcé" par le Responsable du Traitement et qui n'a pas été donné librement par la personne concernée pour les motifs suivants :

2.2.1. Déséquilibre manifeste

Le considérant 43 du RPGD clarifie les situations dans lesquelles le consentement ne peut être considéré comme ayant été librement donné:

> *"Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, (...) et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. ...".*

Bien que le considérant concerne particulièrement les autorités publiques, il n'exclut pas d'autres situations où un déséquilibre similaire entre le responsable du traitement et la personne concernée pourrait être constaté, y compris dans les cas où les responsables de traitements sont des sociétés privées (Groupe de Travail de l'Article 29, Lignes directrices sur le consentement en vertu du Règlement 2016/679 (WP259), page 7):

> *"Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant*

2.2. Freely given consent

Consent can only be a lawful ground for processing if data subjects are offered a genuine and realistic choice to accept or decline the terms of a service or to decline these terms without detriment. In other words, consent will not be valid, if the data subject has no genuine or real choice, feels compelled to consent or will endure negative consequences if they do not consent, as mentioned in the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259) from 10 April 2018.

The controller has carried out unlawful processing of the data subject's personal data, infringing the GDPR. This unlawful processing is based on consent that was "*forced*" by the controller and not freely given by the data subject, on the following grounds:

2.2.1. Clear imbalance of power

Recital 43 of the GDPR clarifies situations in which consent cannot be seen as freely given:

> *"...consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller (...) and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."*

Although the Recital is particularly concerned with authorities, it does not exclude other situations where a similar imbalance of powers between the controller and the data subject might arise, including situations where controllers are private corporations (Article 29 WP Guidelines on consent under Regulation 2016/679 (WP259), page 7):

> *"Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she*

negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will."
[Aucune traduction française disponible actuellement]

Lorsqu'un responsable de traitement se trouve dans une position dominante créant un déséquilibre manifeste entre lui et la personne concernée, un tel déséquilibre est susceptible d'affecter le caractère volontaire du consentement de cette dernière pour le traitement de données à caractère personnel.

Position dominante sur le marché
Il ne peut être contesté que le Responsable du Traitement a une position dominante sur le marché en matière de systèmes d'exploitation de smartphones et la seule concurrence fait partie d'un duopole. Actuellement, environ 85% des smartphones mondiaux utilisent Android et environ 15% utilisent iOS d'Apple, Inc. Il n'existe pas d'alternative réaliste à ces deux systèmes d'exploitation.

Effet des écosystèmes
Compte tenu de la position dominante du Responsable du Traitement sur le marché et du fait que le logiciel du Responsable du Traitement est un logiciel fermé et, pour certaines de ses parties, un logiciel propriétaire, la personne concernée est davantage limitée dans son choix car de nombreuses "applications" ou matériels auxiliaires exigent l'utilisation d'un smartphone opérant sous Android (ou iOS). Ainsi, même les applications mobiles des services publics ne sont souvent disponibles que pour les utilisateurs de terminaux équipés d'un système d'exploitation Android ou iOS. Par exemple, l'application mobile de la SNCF n'existe que pour Android et iOS tout comme l'application "ameli" de l'Assurance Maladie française.

Conclusion
La personne concernée ne semble avoir d'autre choix réaliste que de consentir à la politique de confidentialité et aux conditions d'utilisation fournies par le Responsable du Traitement, compte tenu du déséquilibre manifeste existant entre eux. Ne pas consentir entraînerait une conséquence négative significative pour la personne concernée. Par conséquent, tout consentement obtenu de la part de la personne concernée est invalide pour ces seuls motifs.

does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will."

If a controller is in a dominant position that creates an imbalance of power between him and the data subject, then this is likely to affect the voluntariness of the latter's consent for the processing of personal data.

Dominant Market Position
It cannot be disputed that the controller has a dominant market position in the area of smart phone operating systems and the only competition is part of a duopoly. Currently about 85% of global smart phones are using Android and about 15% use iOS by Apple Inc. There are no realistic alternatives to these two systems.

Effect of Ecoysystems
Given the dominant market position of the controller and the fact that the software of the controller is a closed and (in certain parts) a proprietary software, the data subject is further limited in his/her choice, as many "apps" or other auxiliaries require the use of an Android (or iOS) smart phone. Even public services applications are often available for Android or iOS users only. For instance, the SNCF app is only available for Android and iOS users just like the "ameli" app of the French public Health Insurance.

Summary
In summary, the data subject seems to have no other realistic option than to consent to the privacy policy and terms provided by the controller, given the imbalance of power between them. Not consenting would result in a significant negative consequence for the data subject. Consequently, any consent obtained from the data subject is invalid on these grounds alone.

2.2.2. Conditionnalité de l'accès au Service *("à prendre ou à laisser")*

L'article 7(4) du RPGD dispose expressément que pour évaluer si le consentement est libre,

> *"... il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat."*

Le législateur a choisi d'énumérer explicitement la conditionnalité comme un exemple typique de consentement n'ayant pas été donné librement. Par le choix des mots *"entre autres"*, le législateur a précisé que le consentement n'ayant pas été donné librement ne se limite pas aux cas de conditionnalité.

Le considérant 43 du RGPD ajoute :

> *"Le consentement est présumé ne pas avoir été donné librement (...) si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle execution".*

Le but de cette disposition est de garantir que les services ne sont pas proposés à condition que les personnes concernées fournissent des données à caractère personnel aux responsables de traitements, une telle communication n'étant pas nécessaire pour la mise à disposition de ces services.

Le consentement tout comme le contrôle exercé par tout individu sur les données à caractère personnel qu'il transmet sont en effet vidés de leur sens si les services ne sont offerts qu'en échange d'un consentement obligatoire à l'exploitation de ses données à caractère personnel.

Dans l'affaire C-291/12 (Michael Schwarz contre Stadt Bochum), la Cour de justice de l'Union européenne a examiné la validité de la législation de l'UE prévoyant la prise obligatoire d'empreintes digitales lors de la délivrance de passeports. La Cour a noté au paragraphe 32:

> *« En ce qui concerne, tout d'abord, la condition tenant au consentement des demandeurs de passeports avec le prélèvement de leurs empreintes digitales, il convient de relever que la possession d'un passeport est, en règle générale,*

2.2.2. Conditional for service ("*take it or leave it*")

Article 7 (4) of the GDPR expressly stipulates that to assess whether consent is freely given

> "*...utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*".

The legislator chose to explicitly list conditionality as an illustrative example of not freely given consent. By the choice of the words "*inter alia*", the legislator clarified that not freely given consent is not limited to cases of conditionality only.

Recital 43 of the GDPR further specifies:

> *"Consent is presumed not to be freely given (...) if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."*

The purpose of this provision is to ensure that services are not offered upon the condition that data subjects provide personal information to controllers, such a communication being unnecessary for the offering of these services.

Consent as well as individuals' control over the personal data they provide would be indeed deprived of any meaning, if services are only offered in exchange for mandatory consent to the exploitation of personal data.

In *C-291/12* (*Michael Schwarz v Stadt Bochum*), the Court of Justice of the European Union considered the validity of EU law providing for the mandatory taking of fingerprints when issuing passports. The Court noted in paragraph 32:

> *"First of all, concerning the condition requiring the consent of persons applying for passports before their fingerprints can be taken, it should be noted that, as a general rule, it is essential for citizens of the Union to own a passport in order, for example, to travel to non-member countries and that*

indispensable aux citoyens de l'Union notamment pour effectuer des déplacements à destination de pays tiers et que ce document doit contenir des empreintes digitales, en application de l'article 1er, paragraphe 2, du règlement no 2252/2004. Ainsi, les citoyens de l'Union souhaitant effectuer de tels déplacements ne peuvent s'opposer librement au traitement de leurs empreintes digitales. Dans ces conditions, les demandeurs de passeports ne sauraient être considérés comme ayant consenti à un tel traitement ».

Alors que ce jugement portait sur une autorité publique, des situations similaires de liberté limitée sont également fréquentes dans le secteur privé. En particulier, le fait de devoir «*payer*» des informations à caractère personnel ou d'être refusé des services essentiels est contraire aux principes énoncés dans le RGPD. Comme le Groupe de travail de l'Article 29 l'a déjà noté à la page 8 de sa communication WP 259:

> *"GDPR ensures, that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."* [Pas de traduction française disponible actuellement]

Ces pratiques sont d'ailleurs combattues par une grande majorité d'Européens. Plus précisément, le Flash Eurobaromètre 443 de la Commission européenne (e-Privacy, décembre 2016, page 5) montre que 64% des personnes interrogées trouvent *«inacceptable que leurs activités en ligne soient surveillées en échange d'un accès illimité à un certain site Web»*.

Par conséquent, le consentement allégué de la personne concernée est également invalide pour ces motifs.

2.2.3. Spécificité *("Tout ou rien")*

Le Responsable du Traitement exige de la personne concernée de consentir à sa politique de confidentialité et à ses conditions d'utilisation dans leur ensemble, ce qui qui couvre en fait tous les "services", que le Responsable du Traitement met à disposition (par exemple YouTube, le navigateur Chrome, Google Services, Google Maps, Google Search, Google Actualités, Gmail, AdWords tout comme plusieurs autres services). Malgré le fait que la plupart de ces services n'ont jamais été utilisés par la personne concernée, celle-ci doit tout de même potentiellement accepter leurs conditions d'utilisation également et donc permettre l'exploitation de ses

that document must contain fingerprints pursuant to Article 1(2) of Regulation No 2252/2004. Therefore, citizens of the Union wishing to make such journeys are not free to object to the processing of their fingerprints. In those circumstances, persons applying for passports cannot be deemed to have consented to that processing."

While this judgement was dealing with a public authority, similar situations of limited freedom are common in the private sector as well. In particular, being forced to "*pay*" with personal information or otherwise being denied crucial services is contrary to the principles enshrined in the GDPR. As the Article 29 Working Party has already noted on page 8 of WP 259:

> *"GDPR ensures, that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."*

These practices are, moreover, opposed to by a large majority of Europeans. Specifically, the European Commission's Flash Eurobarometer 443 (e-Privacy, December 2016, page 5) shows that 64% of respondents find it *"unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website*".

Consequently, the data subject's alleged consent is also invalid on these grounds.

2.2.3. Granularity ("*all or nothing*")

The controller requires the data subject to consent to the privacy policy and to the terms as a whole, which in fact cover all the "services", that the controller offers (e.g. YouTube, Chrome Browser, Google Services, Google Maps, Google Search, Google News, Gmail, AdWords, as well as several other services). Despite the fact that most of these services have never been used by the data subject, the latter still has to potentially agree to their terms too, allowing the processing of his/her personal data.

données à caractère personnel.

Le Responsable du Traitement s'appuie donc sur un accord global pour les smartphones opérant le système d'exploitation Android, mais également pour des dizaines d'autres produits. Il s'agirait donc d'un consentement invalide car un tel consentement ne saurait en aucun cas être qualifié de « *spécifique* ». En effet, le consentement donné en l'espèce relève davantage d'une approche de «tout ou rien».

Le considérant 43 du RGPD précise en outre que le consentement ne peut pas être présumé comme ayant été donné librement,

> *"... si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce".*

Si le Responsable du Traitement, au cours de cette procédure de plainte, soutient qu'il existe un acte de consentement plus spécifique, il lui sera toujours nécessaire de démontrer que chaque opération de traitement ou ensemble d'opérations de traitement est fondé sur un acte de consentement spécifique. Compte tenu de la description vague et peu claire du fondement juridique sur lequel le Responsable du Traitement s'appuie, nous ne sommes pas en mesure de commenter cette question à ce stade.

2.2.4. Sans préjudice

Comme expliqué au considérant 42 du RGPD, le Responsable du Traitement doit démontrer que la personne concernée a la possibilité de refuser de donner son consentement sans préjudice.

À la page 11 de ses lignes directrices sur le consentement en vertu du règlement 2016/679 (WP259), le Groupe de Travail de l'Article 29 donne l'exemple de la «rétrogradation» d'un service lorsque le consentement n'est pas donné.

Dans le cas présent, le Responsable du Traitement ne met simplement aucun service à disposition sans forcer préalablement la personne concernée à accepter ses conditions d'utilisation et sa politique de confidentialité. Or être privé d'utilisation de l'un de ces services pourrait être perçu comme quelque chose de bien pire que le fait de devoir utiliser une version antérieure de ce dernier.

The controller therefore relies on an overall bundled consent to anything contained in the privacy policy for Android phones, which includes several other products. This would also render consent invalid, as such consent would not be in any way "*specific*", but rather based on an "*all or nothing*" approach.

Recital 43 of GDPR further clarifies that consent cannot be presumed to be freely given,

> *"...if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case"*

Should the controller in the course of this procedure argue that there is a more specific act of consent, he would still be required to demonstrate that each processing operation or set of processing operations is based on a specific act of consent. Given the vague and unclear description of the legal basis that the controller relies on, we are unable to comment on this issue at this point.

2.2.4. Without detriment

As explained in Recital 42 of the GDPR the controller has to demonstrate, that the data subject has the possibility to refuse consent without detriment.

On page 11 of its Guidelines on consent under Regulation 2016/679 (WP259) the Article 29 Working Part gives the example of "downgrading" a service when consent is not given, as a situation where there is a detriment to the data subject.

In the present case, the controller simply does not offer any service without data subject's first agreeing to the terms and to the privacy policy. Being denied the use of any of these services could be seen as something worse than the simple downgrading of a service.

Compte tenu de la position dominante du Responsable du Traitement et de la popularité du service, cela entraîne également un inconvénient secondaire pour la personne concernée : outre le fait de ne pas pouvoir utiliser le service, la personne concernée perdrait également une forme cruciale d'interaction sociale sans smartphone.

2.2.5. Conclusion

Le Responsable du Traitement ne saurait invoquer le prétendu "consentement", tel que décrit à la section 1.4, car ce consentement enfreint toutes les exigences particulières énoncées à l'article 4(11), à l'article 6(1)(a), à l'article 7 et/ou à l'article 9(2)(a) du RGPD, ainsi que tous les éléments identifiés par les lignes directrices du Groupe de Travail Article 29. Toute opération de traitement basée sur un tel "consentement forcé" constitue donc une violation des droits de la personne concernée en vertu du RGPD.

Given the position of the controller and the popularity of the service, this also leads to a secondary disadvantage for the data subject: In addition to not being able to use the service, the data subject would also lose a crucial form of social interaction without a smart phone. Such a situation is worse than a downgrading.

2.2.5. Summary

In summary, the controller cannot rely on the alleged "consent", as described under section 1.4, as such consent infringes all the particular requirements set out in Article 4(11), Article 6(1)(a), Article 7 and/or Article 9(2)(a) of the GDPR, as well as all elements identified by the Article 29 Working Party Guidelines. Any processing operation that is based on such "forced consent" breaches the rights of the data subject under the GDPR.

2.3. À titre subsidiaire, si l'Autorité de Contrôle ne souscrivait pas aux principaux motifs de cette plainte comme l'y invite 2.2.5

Si l'Autorité de Contrôle (contrairement aux arguments ci-dessus) estime que le responsable du traitement a obtenu un consentement "*libre*", la personne concernée invoque les griefs supplémentaires suivants pour lesquels le responsable du traitement n'a pas obtenu un consentement valable pour les opérations de traitement entrant dans le cadre de cette plainte:

2.3.1. Un consentement non „éclairé"

La politique de confidentialité du Responsable du Traitement résume globalement tous les types de données qui peuvent être collectées par le Responsable du Traitement, tous les produits possibles (plus de 30), toutes les finalités envisageables de traitement de ces données, quatre motifs juridiques sur lesquels le Responsable du Traitement peut s'appuyer ainsi qu'un grand nombre de destinataires potentiels de ces données. Ceci est accompagné par des libellés colorés et des exemples, lesquels sont généralement destinés à faire apparaître ces déclarations très larges comme étant plus acceptables, sans pour autant limiter la portée des phrases cruciales en aucune façon.

Autrement dit, la politique de confidentialité pourrait être résumée comme *«traiter toute donnée, à quelque fin que ce soit, pour l'un des quatre motifs juridiques que ce soit, pour l'un de nos produits, quel que soit ce dernier »*.

2.3. In the alternative, should the Supervisory Authority not join the main grounds for this complaint in 2.2.5.

Should the Supervisory Authority (contrary to the arguments above) take the view that the controller obtained "*freely*" given consent, the data subject relies on the following additional grounds why the controller did not obtain valid consent for the processing operations that are within the scope of this complaint:

2.3.1. Not "informed"

The privacy policy of the controller is in essence summarising all types of data that may be processed by the controller, all possible products (more than 30), all possible purposes for processing such data, four legal grounds that the controller may rely on and a wide number of possible recipients. This is accompanied by colourful wording and examples, which are usually intended to make these very broad statements seem more reasonable, while not limiting the breath of the crucial sentences in any way.

In other words, the policy could be summarised as "*processing any data, for any purpose, on any of four legal grounds, for any of our products*".

Même si un avocat qualifié lisait tout le texte fourni par le Responsable du Traitement, il resterait à deviner quelles données sont traitées, dans quel but précis et sur quelle base légale. Cela est intrinsèquement non transparent et inéquitable au sens des articles 5(1)(a) et 13(c). Cette approche contraste donc manifestement avec la notion de *consentement éclairé* ainsi qu'avec l'obligation d'employer des *«termes clairs et simples»* ou même *«faciles à comprendre»* (Considérant 39).

2.3.2. L'absence de spécificité

L'absence de spécificité s'imbrique avec la question du consentement «éclairé». La personne concernée a été contrainte de donner un consentement non spécifique à toute opération de traitement contenue dans la politique de confidentialité du responsable du traitement, ce qui signifie que le consentement allégué n'était pas «spécifique».

2.3.3. Le consentement n'apparaît pas sous une forme distincte de la politique de confidentialité et des conditions d'utilisation du service

L'approche du responsable du traitement consiste à « noyer » le consentement au sens de l'article 6(1)(a) du RGPD dans une longue politique de confidentialité qui apparaît rassembler, d'une part, des informations qui doivent être fournies conformément à l'article 14 du RGPD et, d'autre part, des informations juridiquement non pertinentes qui rappellent davantage la lecture d'une page "d'aide". Cela est clairement contraire à l'article 7(2) qui exige que le consentement soit clairement différencié de ces autres informations.

2.3.4. Une tromperie fondée uniquement sur le consentement et l'ambiguïté du fondement juridique

Le responsable du traitement a en fait invoqué un certain nombre de motifs juridiques en vertu de l'article 6(1) du RGPD, mais a donné à la personne concernée l'impression qu'il s'appuie uniquement sur le consentement en exigeant de celle-ci qu'elle accepte la politique de confidentialité (voir ci-dessus).

Demander le consentement à une opération de traitement, lorsque le Responsable du Traitement s'appuie en réalité sur une autre base juridique, est fondamentalement injuste, trompeur et non-transparent au sens de l'article 5(1)(a), du RGPD, comme le soulignent les Lignes directrices du Groupe de Travail Article 29 concernant le consentement en vertu du Règlement 2016/679 (WP259) (page 23):

> *"Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals."* [Traduction française non disponible]

Even if a trained lawyer reads all the text that the controller provides, he/she is left guessing what data is processed, for which exact purpose and on which legal basis. This is inherently non-transparent and unfair within the meaning of Articles 5(1)(a) and 13(c). This approach therefore stands in clear contrast to the notion of *informed* consent and to the requirements to use any form of "*plain language*" or even "*easy to understand*" (Recital 39).

2.3.1. Not Specific

Interlocked with the issue of "informed" consent, the data subject was forced to give an unspecific consent to any of the processing operations that were contained in the privacy policy of the controller, meaning that the alleged consent was not "*specific*".

2.3.1. Consent not distinguished from privacy policy and terms of service

The approach of the controller "drowns " consent under Article 6(1)(a) of GDPR in a long privacy policy that seems deal with information that must be provided under Article 14 of GDPR, as well as legally irrelevant information that rather reminds the readers of a "help" text. This clearly violates Article 7(2), which requires that consent must be clearly distinguishable from such terms.

2.3.2. Misrepresentation to rely solely on consent and uncertainty about the legal basis

The controller has in fact relied on a number of legal grounds under Article 6(1) of the GDPR, but has given the data subject the impression, that he solely relies on consent, by requesting the data subject to agree to the privacy policy (see above).

Asking for consent to a processing operation, when the controller relies in fact on another legal basis is fundamentally unfair, misleading and non-transparent within the meaning of Article 5(1)(a) of the GDPR, as underlined by the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259) (page 23):

> *"Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals."*

2.4. La possibilité d'actes de consentement antérieurs

Comme précisé au Considérant 171, le responsable du traitement peut fonder les opérations de traitement sur un consentement donné avant le 25 mai 2018, uniquement si le consentement précédent était conforme aux exigences actuelles du RGPD. Il se peut qu'il y ait eu des actes de consentement antérieurs de la personne concernée, mais aucun d'entre eux n'était plus conforme au RGPD que ce que l'acte de consentement allégué décrit dans cette plainte. Les actes de consentement antérieurs sont donc également invalides et donc non pertinents.

3. DEMANDES

3.1. Demande d'enquête

La personne concernée vous demande par la présente (ou nous demandons à toute autre autorité de contrôle avec laquelle vous pourriez coopérer en vertu du chapitre VII du RGPD) d'enquêter pleinement sur cette plainte, conformément aux pouvoirs qui vous sont conférés y compris par l'article 58(1)(a), (e) et (f) du RGPD, afin de déterminer notamment:

(i.) les opérations de traitement effectuées par le responsable du traitement, en relation avec la personne concernée,
(ii.) à quelle fin ces opérations de traitement sont effectuées
(iii.) sur quel fondement juridique pour chaque opération de traitement spécifique le responsable du traitement s'appuie,
(iv.) nous demandons, en outre, qu'une copie de tout registre des activités de traitement (article 30 du RGPD) soit transmise.

Enfin, nous souhaitons demander que les résultats de cette enquête nous soient communiqués au cours de cette procédure, conformément à l'article 77(2) du RGPD et que notre droit d'être entendus en vertu du droit procédural national applicable soit respecté.

3.2. Demande d'interdiction des traitements visés

Nous demandons en outre que vous (ou toute autre Autorité de Contrôle compétente) preniez les mesures nécessaires conformément aux pouvoirs qui vous sont conférés y compris par l'Article 58(1)(d),(f) et (g) du RGPD

2.4. Possible previous acts of consent

As clarified in Recital 171, the controller may base processing operations on consent that was given before 25 May 2018, only if the previous consent complied with the current requirements in GDPR. There may have been previous acts of consent by the data subject, but none of them was in any aspect more compliant with GDPR than the alleged act of consent described in this complaint. Previous acts of consent are equally invalid and therefore irrelevant.

3. APPLICATIONS

3.1. Request to investigate

The data subject hereby requests that you (or any other supervisory authority that you may cooperate with under chapter VII of GDPR) fully investigate this complaint, in accordance with the powers vested in you, including by Article 58(1)(a), (e) and (f) of the GDPR, to particularly determine:

(i.) which processing operations the controller engages in, in relation to the data subject,
(ii.) for which purpose they are performed,
(iii.) on which legal basis for each specific processing operation the controller relies on, and
(iv.) that a copy of any records of processing activities (Article 30 of the GDPR) are acquired.

Finally, we would like to request that the results of this investigation are made available to us in the course of this procedure, in accordance with Article 77(2) of the GDPR and the right to be heard under the applicable national procedural law.

3.2. Request to prohibit the relevant processing operations

We further request that you (or the relevant supervisory authority) take the necessary steps, in accordance with the powers vested in you, including by Article 58(1)(d), (f) and (g) in combination with Article 17 of the GDPR,

en liaison avec l'Article 17 du RGPD afin de faire cesser toute opération de traitement qui serait basée sur un consentement invalide de la personne concernée.

3.3. Demande d'imposition d'amendes efficaces, proportionnées et dissuasives

Enfin, nous demandons à ce que vous (ou l'Autorité de Contrôle compétente), en vertu des pouvoirs prévus à l'article 58(1)(i) en combinaison avec l'article 83(5) du RGPD, infligiez une amende effective, proportionnée et dissuasive contre le responsable du traitement, en tenant compte du fait que:

i. la personne concernée n'est qu'un des millions d'utilisateurs concernés (Article 83(2)(a));
ii. le responsable du traitement a volontairement et intentionnellement violé les exigences de consentement imposées par le RGPD en profitant de sa position dominante et en forçant les personnes concernées à accepter l'utilisation du service, annulant ainsi leur consentement (article 83(2)(b));
iii. le responsable du traitement doit avoir pris connaissance des lignes directrices du Groupe de Travail «Article 29» concernant le consentement au titre du règlement 2016/679 (WP259), mais a choisi de les ignorer (article 83(2)(b));
iv. le responsable du traitement, malgré ses vastes capacités organisationnelles et techniques en tant qu'entreprise multinationale, a choisi de contourner résolument les exigences de traitement de la nouvelle loi, en n'assurant pas, même de la façon la plus indirecte le consentement «libre» (article 83(2)(c));
v. le responsable du traitement traite des données très sensibles, y compris des catégories particulières de données à caractère personnel (article 83(2)(g));
vi. le responsable du traitement n'a apparemment pas l'intention de se conformer au RGPD ni de notifier une autorité de contrôle de cette infraction, cette violation doit donc vous être communiquée au moyen d'une plainte officielle (Article 83(2)(h);
vii. le but de cette infraction était d'obtenir, directement et indirectement, des avantages financiers (par exemple par le biais d'activités de marketing et de publicité); et que

to stop any processing operations that are based on invalid consent by the data subject.

3.3. Request to impose effective, proportionate and dissuasive fines

Finally, we request that you (or the relevant supervisory authority), by virtue of the powers provided by Article 58(1)(i) in combination with Article 83(5) of the GDPR, impose an effective, proportionate and dissuasive fine against the controller, taking into account that:

i. the data subject is only one of the millions of affected users (Article 83(2)(a));
ii. the controller wilfully and intentionally breached the consent requirements imposed by the GDPR, by taking advantage of its dominant position and by forcing data subjects to agree to the use of the service, negating thus their consent (Article 83(2)(b));
iii. the controller must have known about the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), but chose to ignore them (Article 83(2)(b));
iv. the controller, despite its vast organizational and technical capabilities as a multinational company, chose to bluntly circumvent the processing requirements of the new law, by not even remotely ensuring "free" consent (Article 83(2)(c));
v. the controller processes highly sensitive data, including special categories of personal data (Article 83(2)(g));
vi. the controller has apparently no intention to either comply with the GDPR or notify any supervisory authority of this infringement, and this infringement has to therefore be communicated to you by means of a formal complaint (Article 83(2)(h));
vii. the aim of this infringement was to gain, both directly and indirectly, financial benefits (e.g. through marketing and advertising activities); and that
viii. a wilful, massive and profound violation by a major player within the data industry must be adequately sanctioned to prevent similar violations of the GDPR in the future, and to ensure respect of the data subjects' rights under the new data protection acquis.

viii. une violation délibérée, massive et profonde par un acteur majeur de l'industrie des données doit être sanctionnée de manière adéquate pour empêcher des violations similaires du RGPD à l'avenir et garantir le respect des droits des personnes concernées par le nouvel acquis en matière de protection des données.

Selon nos informations, les revenus actuels du groupe Alphabet, dont le Responsable du Traitement est membre, s'élevaient à environ 101,85 milliards de dollars (environ 94,79 milliards d'euros) pour l'exercice de l'année fiscale 2017. L'amende maximale possible en vertu de l'article 83(5)(a) sur la base de 4% du chiffre d'affaires mondial, s'élèverait ainsi à environ 3,79 milliards d'euros.

4. AUTRES

4.1. Traduction anglaise

Étant donné que différentes autorités de contrôle traiteront très probablement ce cas, nous avons pris l'initiative inhabituelle de vous fournir une traduction anglaise informelle de cette plainte. En cas de conflit dans les traductions, la version française devrait prévaloir puisque la loi nous oblige à déposer cette plainte en France auprès de l'Autorité de Contrôle française (Commission Nationale Informatique et Libertés dite "*CNIL*") en français.

4.2. Contact

[redacted]

According to our information the current revenue of the Alphabet Group, of which the controller is a member, was about $ 101.85 billion (about € 94.79 Billion) in the fiscal year 2017. The possible maximum fine under Article 83(5)(a), based on 4% of the worldwide revenue, would accordingly be about € 3.79 billion.

4. OTHER

4.1. English Translation

As different supervisory authorities will most likely deal with this case, we have taken the unusual step to provide you with an informal English translation of this complaint. If there is any conflict in the translations, the French version should prevail, since the law requires us to file this complaint in France with the French Supervisory Authority ("*CNIL*") in French.

4.2. Contact details

[redacted]