noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

CNIL
3 Place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
FRANCE

Par le service des plaintes de la CNIL

Vienne, 14.09.2023

noyb Case-No : C[redacted]

Plaignante : [redacted]

représentée en vertu de l'article 80(1) RGPD par : *noyb* - Centre européen pour les droits numériques
Goldschlagstraße 172/4/3/2, AT-1140 Vienne, Autriche

Défenderesse : **FNAC DARTY PARTICIPATIONS & SERVICES RCS** Créteil 775 661 390 et
FNAC DIRECT RCS Créteil 377 853 536
Le Flavia, 9 rue des Bateaux-lavoirs,
94768 Ivry-sur-Seine, France

et toute autre entité que l'Autorité jugera responsable des violations

Concerne : Violation de l'article 5(3) de la directive « vie privée et communications électroniques »,
Violation de l'article 82 de la loi informatique et libertés,
Violation des articles 5(1) (a), 6(1)(a) et 25(1) et (2) RGPD.

PLAINTE

1. REPRESENTATION

1. *noyb* - European Center for Digital Rights est une organisation à but non lucratif active dans le domaine de la protection des droits et libertés des personnes concernées, dont le siège social est situé Goldschlagstraße 172/4/2, 1140 Vienne, Autriche, numéro d'enregistrement ZVR : 1354838270 (ci-après : « *noyb »)* (pièce 1 « noyb statutes »).

2. *noyb* représente la plaignante en vertu de l'article 80, paragraphe 1, du RGPD (pièce 2 « Convention de Representation »).

2. FAITS RELATIFS A L'AFFAIRE

3. Le responsable du traitement, FNAC, est un magasin en ligne français d'électronique. Le responsable du traitement décrit son application mobile (ci-après « application mobile » ; « application ») : « *Entièrement pensée pour vous et d'après vos retours, l'appli Fnac a été conçue pour vous fournir une expérience d'achat simple, pratique, agréable et comme toujours 100% sécurisée. »*[1] L'application permet essentiellement aux utilisateurs de naviguer dans le magasin et de passer une commande.

2.1. Appareil et données personnelles de la Plaignante

4. La plaignante a installé l'application mobile Fnac du responsable du traitement sur son téléphone, un Samsung S9+ [redacted], le [redacted] à partir de Google PlayStore. Elle était connectée au PlayStore avec son compte Google [redacted].

5. Le téléphone de la Plaignante fonctionne avec le système d'exploitation Android 10 [redacted] (ci-après « OS »). Les spécifications exactes du système d'exploitation sont les suivantes (voir la pièce 3 « Methodology » pour les détails du système d'exploitation) :
   [redacted]

6. Dans le contexte de cette plainte, Google Play Services a été remplacé par MicroG[2]. Contrairement à Google Play Services, MicroG ne renvoie jamais le même identifiant publicitaire Android (ci-après « AdID »). Chaque fois qu'une application mobile le lit, un nouvel AdID est généré et renvoyé. En d'autres termes, si une application mobile donnée lit l'AdID trois fois, le système d'exploitation renverra trois identifiants publicitaires différents. L'AdID unique émis pour l'application Fnac était : [redacted].

7. Le téléphone a été connecté au réseau mobile [redacted] avec le numéro de téléphone : [redacted]. Le numéro de téléphone est enregistré au nom de la plaignante.

[1] Google PlayStore : https://play.google.com/store/apps/details?id=fr.fnac.com&gl=FR (pièce 19 « Fnac Google PlayStore »).

[2] https://microg.org/

2.2. Trafic entre l'application mobile du responsable du traitement et la société de suivi

8. Le [redacted] entre [redacted] et [redacted] (ci-après « la Période pertinente »), le Requérant a utilisé l'application mobile Fnac. La Période pertinente a été déterminée par le premier lancement de l'application et sa fermeture ultérieure (voir la pièce 3 pour la documentation technique complète et la méthodologie, et la pièce 4 « Enregistrement d'écran » pour un enregistrement d'écran de l'utilisation de l'application par la Plaignante pendant la Période pertinente).

9. Immédiatement après le premier lancement de l'application, une bannière a été présentée à la Plaignante. Une capture d'écran de cette bannière est jointe à la pièce 5 « Capture d'écran de la bannière ».

10. La plaignante n'a pas interagi avec la bannière ni avec l'application de quelque manière que ce soit (c'est-à-dire qu'elle n'a pas cliqué sur l'écran du téléphone) (voir pièce 4), si ce n'est pour fermer l'application.

11. L'application Fnac comprend des kits de développement logiciel[3] (ci-après « SDK »), dont l'un appartient à la société d'analytique des utilisateurs Batch[4] (ci-après « société de suivi » ; « Destinataire ») (pièce 6 « Rapport Exodus »).

12. Selon Exodus Privacy, Batch fournit des services d'analytique et de profilage[5]. Selon les propres termes de Batch : « *Batch est LA plateforme d'engagement des clients de la prochaine génération. Nous aidons à créer des relations entre les clients et leurs marques préférées, grâce à une expérience très personnalisée* » *(original : « Batch is THE next-generation Customer Engagement Platform. We help create relationships between customers and their favourite brands, through a very personalized experience »)*. [6]

13. En d'autres termes, Batch offre aux développeurs d'applications des procédés analytiques sophistiqués des utilisateurs. Sur la base de ces analyses, Batch permet à ses clients d'envoyer aux utilisateurs de leurs applications des messages personnalisés, généralement à des fins de marketing[7] .

14. Batch elle-même fournit un exemple de la façon dont elle a aidé Fnac à générer 214,000 euros par une notification push marketing annonçant la précommande de la nouvelle Nintendo Switch à la Fnac (voir la capture d'écran ci-dessous).

---

[3] Un logiciel qui peut être incorporé dans un autre logiciel à des fins fonctionnelles ou publicitaires.

[4] Voir la liste complète fournie par Exodus Privacy : https://reports.exodus-privacy.eu.org/en/reports/fr.fnac.com/latest/ consulté le 25.06.2023 ; pièce 6 « Rapport Exodus ».

[5] Tel que fourni par Exodus Privacy : https://reports.exodus-privacy.eu.org/en/trackers/23/, consulté le 25.06.2023.

[6] Traduction libre ; https://help.batch.com/en/articles/1622557-what-is-batch, consulté le 26.06.2023 ; pièce 7 « What is Batch ».

[7] Voir une « liste non exhaustive » des objectifs du Batch SDK : https://help.batch.com/en/articles/4393095-what-purpose-is-batch-sdk-serving (pièce 8 « What purpose is Batch SDK serving »). Voir aussi : https://batch.com/about (pièce 9 « Batch About »), consulté le 08.08.2023.

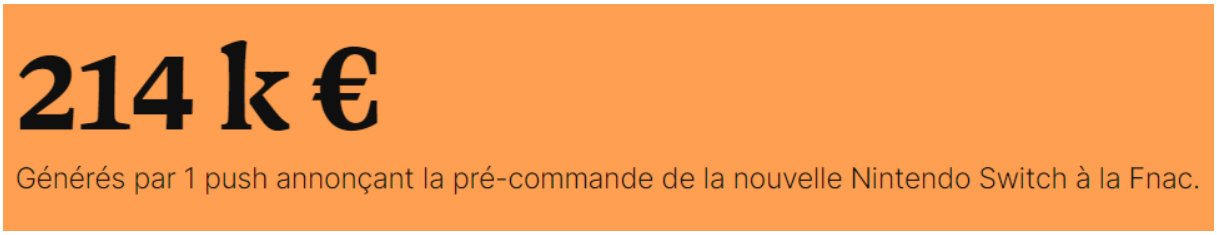


Figure 1. Batch.com : « Why Retailers go with Batch »[8] , consulté le 15 juin 2023.

15. Batch traite donc des données à caractère personnel pour le compte du responsable du traitement et est considéré comme le sous-traitant du responsable du traitement en vertu de l'article 4(8) RGPD.

16. Selon la documentation de Batch destinée aux développeurs, le SDK de Batch recueille par défaut l'AdID des utilisateurs et les données avancées de l'appareil[9] . En intégrant le code « par défaut » de la bibliothèque de suivi spécifiée, l'application Fnac accède par défaut aux données de ses utilisateurs par l'intermédiaire du SDK et les partage avec la société de suivi Batch à des fins d'analyse et de profilage des utilisateurs.

17. Au cours de la Période pertinente, le Requérant a constaté que l'application Fnac envoyait de multiples requêtes[10] (ci-après « Traffic ») contenant les données personnelles de la Plaignante vers des serveurs appartenant à Batch (pièce 12 « Rapport Colander »).

18. Les données transmises comprenaient : l'AdID, modèle d'appareil, marque de l'appareil, version du système d'exploitation et autres identifiants d'utilisateur générés par Batch. L'application Fnac a transmis l'AdID de la Plaignante à la société de suivi Batch cinq fois par minute. Nous fournissons ci-dessous un exemple de transmission de données entre la Fnac et Batch :

[Image redacted]

Figure 2. Exemple de données de trafic de l'application Fnac vers Batch contenant l'AdID, les identifiants personnalisés et les données de l'appareil avancé, [redacted] (voir pièce 12 « Rapport Colander » et pièce 13 « Traffic » pour tous les détails).

19. Un document détaillé de l'ensemble du trafic entre l'application du responsable du traitement et les différents serveurs au cours de la période concernée est joint à la pièce 13 « Traffic ».

3. DROIT APPLICABLE

20. Le stockage de données personnelles et non personnelles sur l'appareil de la Plaignante et l'accès à ces données sont régis par l'article 5(3), de la directive 2002/58/CE concernant la

[8] https://batch.com/customers/retail, (pièce 10 « Why Retailers Go with Batch ») consulté le 08.08.2023.
[9] https://doc.batch.com/android/custom-data/advanced/#advertising-id et https://doc.batch.com/android/custom-data/advanced/#advanced-device-information (pièce 11 « Batch Advanced ») consulté le 12.06.2023.
[10] Message envoyé par un client à un serveur qui contient des informations sur une ressource web, ainsi que sur la manière dont le client souhaite interagir avec cette ressource.

vie privée et les communications électroniques (« directive vie privée et communications électroniques »).

21. La directive « vie privée et communications électroniques » est transposée en France par l'article 82 *de la loi informatique et libertés*, qui transpose l'article 5(3), de ladite directive.

22. Conformément à l'article 5(3), de la directive précitée *«* [...] *le stockage d'informations, ou l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est autorisé qu'à condition que l'abonné ou l'utilisateur concerné ait donné son consentement* [...] *»*. L'article 82 *de la loi informatique et libertés* stipule ce qui suit :

> *Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :*
>
> *1°De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;*
>
> *2° Des moyens dont il dispose pour s'y opposer. Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.*
>
> *Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :*
>
> *1° Soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;*
>
> *2° Soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.*

23. Le traitement ultérieur des données personnelles de la Plaignante, c'est-à-dire la transmission de données personnelles à des tiers à des fins d'analytique et de profilage des utilisateurs, est régi par le RGPD et doit être conforme, entre autres, aux articles 5(1)(a), 6 et 25 du RGPD.

4. AUTORITE COMPETENTE

24. Etant donné que l'établissement principal du responsable du traitement se trouve en France[11], la CNIL est compétente pour examiner cette plainte.

[11] Voir la politique de confidentialité du responsable du traitement : https://www.fnac.com/Help/donneesPersonnelles (pièce 14 « Politique de Protection des Donnees Personnelles Fnac »).

5. CONTEXTE : SUIVI INCONTROLE DANS LES APPLICATIONS MOBILES

25. Un certain nombre d'études ont fait état d'un suivi généralisé et incontrôlé des utilisateurs d'applications mobiles, à leur insu et en violation de la législation applicable[12] .

26. Selon mnemonic[13] , une société norvégienne de cybersécurité, les politiques de confidentialité des applications sont relativement rarement mises à jour, étant donné que les tiers avec lesquels les applications partagent des données changent fréquemment et sont même souvent choisis de manière dynamique, c'est-à-dire sans que le fournisseur de l'application ou la personne concernée n'en aient connaissance à l'avance. Les politiques de confidentialité ne reflètent donc souvent pas la réalité du partage des données.

27. Du point de vue de l'utilisateur, il est donc difficile de comprendre avec qui ses données sont partagées et de les contrôler. Le secteur de la publicité en ligne a été décrite comme étant à l'origine de la « *plus grande violation de données au monde* »[14] .

28. La prévalence de ce modèle de partage des données est confirmée par une étude menée par Kollnig et al : 88,73 % des 12 000 applications Android étudiées et 79,35 % des 12 000 applications iOS échantillonnées contenaient au moins une bibliothèque de traçage (tracking library).[15] L'application moyenne sur les deux plateformes a contacté un nombre similaire de domaines de suivi (2,7 sur Android et 2,4 sur iOS) avant toute interaction avec l'utilisateur. Seules 18,6 % des applications Android et 31,5 % des applications iOS n'ont contacté aucun domaine de suivi au lancement de l'application.[16] 55,4 % des applications Android et 31 % des applications iOS ont partagé l'identifiant publicitaire unique (AdID) du téléphone avec des tiers. 85,1 % des applications Android et 61,4 % des applications iOS ont partagé le modèle et le nom du téléphone, qui contient souvent le prénom et le nom de famille de l'utilisateur du téléphone.[17]

29. D'autres études appuient cette conclusion, notamment une étude menée par l'Institut pour la sécurité des applications de l'Université technique de Braunschweig, qui a révélé que près de 73 % des applications envoyaient des demandes contenant des données personnelles

---

[12] Voir, par exemple, Konrad Kollnig et al : Konrad Kollnig et. al, A Fait Accompli ? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps : https://www.usenix.org/system/files/soups2021-kollnig.pdf (consulté le 13 avril 2023) ; Konrad Kollnig et. al., Before and after RGPD : tracking in mobile apps : https://policyreview.info/articles/analysis/and-after-RGPD-tracking-mobile-apps (consulté le 13 avril 2023) ; Trung Tin Nguyen et. al., Share First, Ask Later (or Never ?) Studying Violations of RGPD's Explicit Consent in Android Apps : https://www.usenix.org/system/files/sec21-nguyen.pdf (consulté le 13 avril 2023) ; Benjamin Altpeter, Worrying confessions : A look at data safety labels on Android : https://www.datarequests.org/blog/android-data-safety-labels-analysis/ (consulté le 13 avril 2023).

[13] Andreas Claesson et Tor E. Bjørstad, Out of Control : A review of data sharing by popular mobile apps, p. 12 : https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf (consulté le 13 avril 2023).

[14] Procès ICCL, 15 juin 2021, https://www.iccl.ie/rtb-june-2021/#press

[15] Kollnig et al, Are Iphones Really Better for Privacy ? A Comparative Study of iOS and Android Apps, 4.1.1, p. 8, 9 : https://arxiv.org/pdf/2109.13722.pdf, (consulté le 13 avril 2023).

[16] Kollnig et al, Are Iphones Really Better for Privacy ? A Comparative Study of iOS and Android Apps, 4.3.1, p. 12 : https://arxiv.org/pdf/2109.13722.pdf, (consulté le 13 avril 2023).

[17] Kollnig et al, Are Iphones Really Better for Privacy ? A Comparative Study of iOS and Android Apps, 4.3.1, p. 12 : https://arxiv.org/pdf/2109.13722.pdf, (consulté le 13 avril 2023).

directement au lancement de l'application, avant toute autre interaction avec l'utilisateur.[18] Les propres recherches du fournisseur de CMP « UserCentrics » montrent également qu' « *neuf applications sur dix collectent des données personnelles auprès des utilisateurs sans leur consentement* ».[19]

30. En outre, selon d'autres recherches[20], 43,7 % des 1 297 applications Android étudiées qui affichaient une bannière contextuelle au lancement de l'application ne proposaient qu'un seul choix, par exemple un bouton intitulé « Accepter la politique et utiliser l'application » ou des cases à cocher obligatoires sans autre alternative. En outre, 20,2 % des applications permettaient aux utilisateurs de donner ou de refuser leur consentement, mais quittaient immédiatement l'application en cas de refus. Seules 3,5 % des applications offraient aux utilisateurs la possibilité de refuser de consentir.[21]

31. En outre, seules 3 des 13 bibliothèques de suivi SDK évaluées intègrent par défaut un mécanisme de collecte du consentement de l'utilisateur, et aucun des cinq trackers les plus courants ne le fait (quatre d'entre eux appartiennent à Google et un à Meta (anciennement Facebook)).[22]

32. Lorsqu'ils ont été informés de violations potentielles du RGPD, de nombreux développeurs d'applications ont répondu qu'ils pensaient que la mise en place d'une politique de confidentialité était suffisante pour présumer du consentement des utilisateurs.[23]

33. Bien que les sociétés de suivi fournissent souvent des conseils aux développeurs sur la conformité au RGPD, ces conseils sont parfois difficiles à trouver, à lire et mal entretenus.[24] Ceci étant dit, il incombe principalement aux développeurs d'applications de s'assurer qu'ils recueillent un consentement valide au regard du RGPD pour le stockage ou l'accès aux informations sur l'appareil de l'utilisateur et pour le traitement ultérieur des données personnelles de l'utilisateur à des fins de suivi.

---

[18] Benjamin Altperter, Technische Universität Braunschweig, Informed Consent ? A Study of 'Consent Dialogs' on Android and iOS, 10, p. 60 : https://benjamin-altpeter.de/doc/thesis-consent-dialogs.pdf (consulté le 13 avril 2023).

[19] Usercentrics (2022) : https://usercentrics.com/press/apps-report/ (consulté le 13 avril 2023).

[20] Kollnig et al, A Fait Accompli ? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps, 4.2, p. 8 : https://arxiv.org/pdf/2106.09407.pdf (consulté le 13 avril 2023).

[21] Kollnig et al, A Fait Accompli ? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps, 4.2, p. 9 : https://arxiv.org/pdf/2106.09407.pdf (consulté le 13 avril 2023).

[22] Kollnig et al, A Fait Accompli ? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps, 5.2, p. 9 : https://arxiv.org/pdf/2106.09407.pdf (consulté le 13 avril 2023).

[23] Nguyen et al, Share First, Ask Later (Or Never ?) Studying Violations of RGPD's Explicit Consent in Android Apps, 5.2, p. 13 : https://www.usenix.org/system/files/sec21-nguyen.pdf (consulté le 13 avril 2023).

[24] Kollnig et al, A Fait Accompli ? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps, 5.2, p. 9, 10 : https://arxiv.org/pdf/2106.09407.pdf (consulté le 13 avril 2023).

6. MOTIFS DE LA PLAINTE

6.1. L'accès aux données de la Plaignante sans son consentement est illégal

34. Le responsable du traitement a accédé aux données de la plaignante qui étaient stockées sur son appareil lorsqu'il les a partagées avec Batch (pièce 13 « Traffic »), ce qui a déclenché l'obligation de consentement en vertu de l'article 5(3) de la directive « vie privée et communications électroniques » et de l'article 82 *de la loi informatique et libertés*.

35. Comme expliqué dans la section 2.2 la plaignante n'a pas interagi avec la bannière qui lui a été présentée au lancement de l'application et n'a pas non plus consenti à l'accès aux données sur son appareil (pièce 4 « Enregistrement d'écran »).

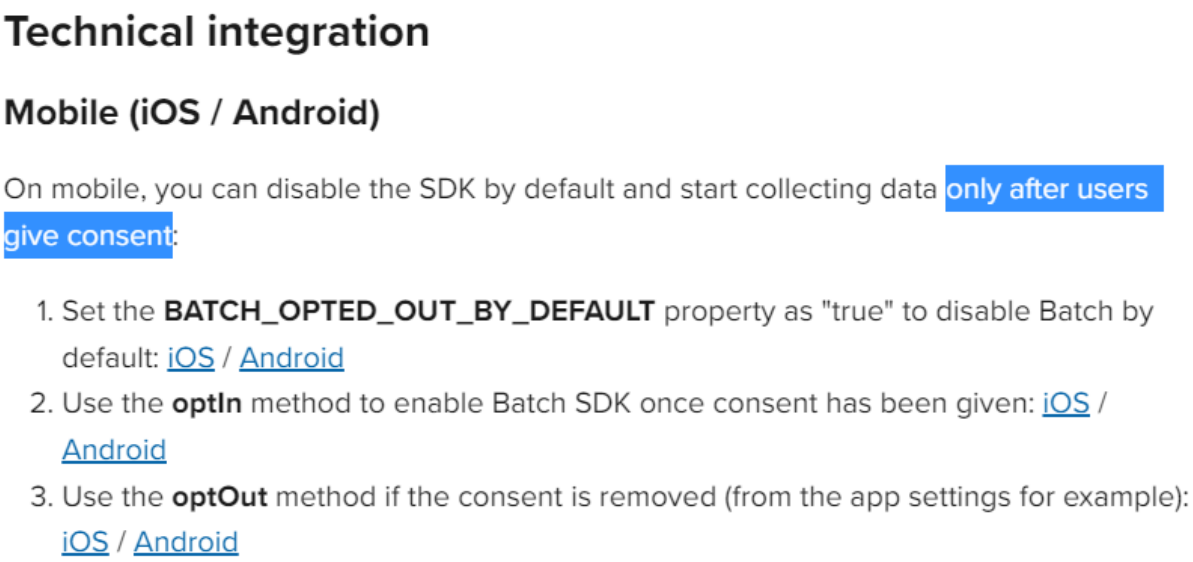
36. L'article 5(3) de la directive « vie privée et communications électroniques » et l'article 82 *de la loi informatique et libertés* prévoient des dérogations spécifiques à l'obligation de consentement lorsque cet accès est techniquement nécessaire à la transmission d'une communication (directive « vie privée et communications électroniques ») ou est « *strictement nécessaire* » (directive « vie privée et communications électroniques » et *loi informatique et libertés*) à la fourniture d'un service de la société de l'information explicitement demandé par l'abonné ou l'utilisateur.

37. Aucune de ces exceptions ne s'applique au cas présent. Les données ont été consultées à des fins d'analytique et de profilage des utilisateurs, ce qui n'est ni l'un ni l'autre strictement nécessaire pour fournir une fonctionnalité explicitement demandée par le plaignant, à savoir l'utilisation de l'application. Les données consultées n'étaient pas non plus techniquement nécessaires pour effectuer la transmission d'une communication.[25]

38. Notons que Batch explique comment intégrer le SDK de manière à ce que les données ne soient collectées qu'avec le consentement de l'utilisateur. Ceci n'est cependant pas le cas en l'espèce.[26]

[25] Voir le projet de recommandations relatives aux applications mobiles de la CNIL, pages 28-29.

[26] https://help.batch.com/en/articles/5204072-how-to-integrate-batch-into-my-cmp (pièce 15 "How to integrate Batch into my CMP") consulté le 12.06.2023. Notons que Batch explique comment intégrer le SDK de manière à ce que les données ne soient collectées qu'avec le consentement de l'utilisateur. Ceci n'est cependant pas le cas en l'espèce.



Technical integration

Mobile (iOS / Android)

On mobile, you can disable the SDK by default and start collecting data only after users give consent:

1. Set the **BATCH_OPTED_OUT_BY_DEFAULT** property as "true" to disable Batch by default: iOS / Android
2. Use the **optIn** method to enable Batch SDK once consent has been given: iOS / Android
3. Use the **optOut** method if the consent is removed (from the app settings for example): iOS / Android

Figure 3. Guide SDK Batch sur l'intégration de Batch dans le CMP (12 juin 2023).

39. Le responsable du traitement a donc violé l'article 5(3) de la directive « vie privée et communications électroniques » et l'article 82 de *la loi informatique et libertés* en accédant aux informations contenues dans l'appareil de la Plaignante sans son consentement.

6.2. Le traitement ultérieur des données de la Plaignante sans son consentement est également illégal

40. Le responsable du traitement a partagé l'AdID, le modèle de l'appareil, la marque de l'appareil et la version du système d'exploitation. L'AdID est un « *identifiant publicitaire est un identifiant unique, réinitialisable par l'utilisateur, pour la publicité* »[27] fourni par le système d'exploitation. L'AdID permet donc d'afficher de la publicité ciblée à l'utilisateur. Par conséquent, étant donné que l'AdID est 1) unique, 2) associé à l'utilisateur (soit par lui-même, soit par regroupement avec d'autres données, telles que le modèle de l'appareil, la marque de l'appareil, la version du système d'exploitation, d'autres identifiants uniques de l'utilisateur), et qu'il permet d'identifier l'utilisateur, il est considéré comme une donnée à caractère personnel au sens de l'article 4(1) RGPD.

41. Même dans les scénarios où le système d'exploitation génère successivement plusieurs identifiants à chaque demande d'accès à l'AdID par l'application, tout AdID traité par le fournisseur de SDK reste une donnée personnelle car il est associé à l'utilisateur. La génération et la transmission de plusieurs AdID ne rompt pas l'association entre l'utilisateur et l'AdID. En outre, les AdID sont rarement transmis au fournisseur de SDK de manière isolée. Ils sont généralement transmis avec d'autres données qui restent inchangées. Enfin, le fournisseur de SDK cherche spécifiquement à relier les différents appareils et profils (c'est ainsi qu'un AdID peut être appelé) des utilisateurs[28].

---

[27] Google Play Console Help: https://support.google.com/googleplay/android-developer/answer/6048248?hl=fr (pièce 17 « Google Advertising ID ») consulté le 26.06.2023.

[28] Voir par exemple https://help.batch.com/en/articles/6441020-how-to-fill-out-the-advertising-id-collection-form-in-the-play-console (pièce 20 « Batch Knowledge base ») consulté le 21.08.2023.

42. Le responsable du traitement a collecté les données à caractère personnel de la Plaignante et les a transmises à la société de suivi Batch à des fins d'analytique et de profilage des utilisateurs. Cela équivaut à un « traitement » au sens de l'article 4(2) RGPD.

43. Conformément à l'article 5(1)(a) du RGPD, le traitement doit être licite, loyal et transparent. Pour se conformer au principe de licéité, le responsable du traitement doit s'appuyer sur l'une des six bases légales prévues à l'article 6 du RGPD.

6.2.1. Les données ont été traitées sans le consentement de la Plaignante, seule base légale pertinente dans le cas d'espèce

44. Comme l'expliquent la documentation et le site web de Batch, Batch est une plateforme d'engagement des clients qui offre aux développeurs d'applications un procédé d'analytique sophistiqué des utilisateurs, y compris un profilage, ainsi que des fonctions de messagerie personnalisée, généralement à des fins de marketing, aux utilisateurs de ces applications sur la base de l'analyse des utilisateurs réalisée.[29]

45. Fnac, en tant que responsable du traitement, doit s'assurer que ce traitement effectué par Batch pour le compte de Fnac est licite. Ce traitement étendu est considéré comme un traitement de données à haut risque et ne doit être effectué qu'après obtention d'un consentement valide au regard du RGPD (article 6(1)(a) du RGPD)[30] .

46. Si un responsable du traitement s'appuie sur le consentement comme base légale pour accéder à des données à caractère personnel, il doit s'appuyer sur la même base légale pour tout traitement effectué en aval dans le même but. Toute autre solution reviendrait à contourner la protection que la directive « vie privée et communications électroniques » cherche à accorder en exigeant l'obtention d'un consentement préalable.

47. Ce point de vue est soutenu par l'EDPB et l'EDPS qui rappellent conjointement :

> « [...] *que lorsque le consentement est requis en vertu de l'article 5, paragraphe 3, de la directive « vie privée et communications électroniques », le consentement au titre de l'article 6 du RGPD constituerait très probablement la base juridique adéquate pour tout traitement de données à caractère personnel consécutif au stockage d'informations ou à l'obtention d'un accès à des informations déjà stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ».*[31]

48. Or dans ce le cas d'espèce, comme déjà développé dans la section 6.2 ci-dessus, et comme confirmé par la CNIL dans son projet de recommandation sur les applications mobile[32], Fnac

---

[29] Voir une « liste non exhaustive » des objectifs du Batch SDK : https://help.batch.com/en/articles/4393095-what-purpose-is-batch-sdk-serving (pièce 8 « What purpose is Batch SDK serving »). Voir aussi : https://batch.com/about (pièce 9 « Batch About »), consulté le 08.08.2023.

[30] Voir par exemple la page 32 de l'avis du WP29 « Opinion 06/2014 on the notion of legitimate interests » (06/2014) et la page 46 de l'avis du WP29 « Opinion 03/2013 on purpose limitation » (03/2013), qui précisent que le profilage et l'analyse requièrent le consentement de la personne concernée.

[31] « Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) », paragraphe 44.

[32] Projet de recommandation relative aux applications mobiles de la CNIL, page 28-29.

doit donc demander à l'utilisateur un consentement valide au regard du RGPD pour traiter ses données personnelles à des fins d'analyse et de profilage de l'utilisateur par l'intermédiaire de Batch.

49. Notamment, Batch elle-même recommande que le responsable du traitement s'appuie sur le consentement pour traiter les données des utilisateurs.[33]

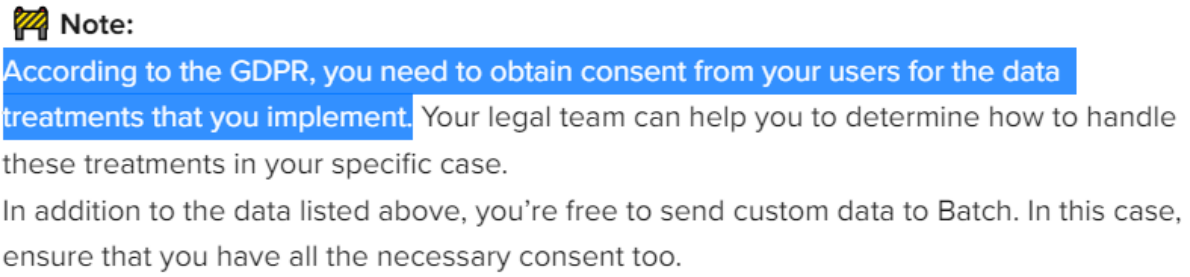


Figure 4. Batch SDK guide « GDPR Compliance » (pièce 16 « Batch GDPR Compliance ») consulté le 11 juin 2023.

50. Le responsable du traitement agit en tant que « première partie » vis-à-vis du plaignant. Cela signifie que la Plaignante interagit directement avec le responsable du traitement lorsqu'il utilise son application. Par conséquent, le responsable de traitement est également responsable de s'assurer qu'il recueille auprès de la Plaignante un consentement valide au sens du RGPD pour partager ses données personnelles avec les tiers dont il intègre les SDK dans l'application mobile.[34]

51. La Plaignante n'a pas donné son consentement (voir section 2.2). En tout état de cause, conformément à l'article 7(1) du RGPD, le responsable du traitement doit démontrer que la plaignante a consenti au traitement de ses données à caractère personnel.

6.3. Les principes de protection des données par défaut et dès la conception (article 25 du RGPD)

52. Comme rappelé par la CNIL dans son projet de recommandation[35], l'éditeur de l'application doit appliquer les principes de protection des donnée par défaut et dès la conception, en application de l'article 25 du RGPD.

53. La documentation de Batch pour les développeurs montre que le SDK de Batch collecte l'AdID et des données avancées du terminal par défaut en dépit du fait que cette collecte nécessite le consentement préalable.[36] Batch aurait pu rendre son code conforme aux exigences légales en n'autorisant la collecte d'AdID qu'à condition qu'un consentement préalable soit donné.

---

[33] Voir également : https://help.batch.com/en/articles/1957231-gdpr-compliance, (pièce 16 « Batch GDPR Compliance ») consulté le 11.06.2023.

[34] Voir dans le même sens la Délibération SAN-2023-009 du 15 juin 2023 concernant la société CRITEO et le communiqué de presse sur https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million, consulté le 03.07.2023.

[35] Projet de recommandation relative aux applications mobiles de la CNIL, page 30, point 3.

[36] https://doc.batch.com/android/custom-data/advanced/#advertising-id; https://doc.batch.com/android/custom-data/advanced/#advanced-device-information; https://doc.batch.com/android/sdk-integration/#advertising-id, consulté le 26.06.2023 (pièce 11 « Batch Advanced »).

Cependant, Batch a décidé d'écrire son code en violant les exigences de la directive « vie privée et communications électroniques » et du RGPD.

54. Il est cependant évident que FNAC n'a pas changé le code par défaut du SDK de Batch en intégrant le code dans l'application puisque la collecte des données a commencé dès que la Plaignante a lancé l'application.

55. En outre, la FNAC a traité l'AdID de la Plaignante pour une finalité analytique (voir section 2.2). Or, un tel traitement n'est pas nécessaire pour la fourniture du service. L'AdID, selon la documentation de Google, est « un identifiant unique et réinitialisable par l'utilisateur qui est utilisé pour la publicité. Il donne davantage de contrôle aux utilisateurs, et constitue un système simple et standardisé pour les développeurs qui veulent continuer à monétiser leurs applications.[37] Il est clair que la finalité de l'AdID est de permettre aux développeurs de monétiser leurs applications à des fins de publicité.

56. Comme le rappelle la CNIL dans son projet de recommandation relative aux applications mobiles, prévoir un traitement qui n'est pas indispensable à la fourniture du service contrevient aux principes de protection des données par défaut et dès la conception.[38]

57. En outre, l'éditeur devrait laisser le choix à l'utilisateur final de choisir d'utiliser ou non les fonctionnalités non strictement nécessaires au bon fonctionnement de l'application.[39]

58. Comme déjà mentionné, le SDK de Batch collecte les données par défaut mais la collection de l'AdID est optionnel et peut être désactivé par le développeur de l'application, selon Batch. [40]

59. En ne désactivant pas la collecte et le traitement par défaut de l'AdID à des fins d'Analytique, et dès lors en permettant une collecte non nécessaire de données, FNAC a dès lors violé le principe de protection des données par défaut et dès la conception.

7. REQUETES

7.1. Demande d'enquête

60. La Plaignante demande votre Autorité de mener une enquête approfondie sur cette plainte, conformément à l'article 58(1) a), e) et f), du RGPD, afin de déterminer, notamment

    a) les opérations de traitement auxquelles se livre le responsable du traitement en ce qui concerne les données à caractère personnel de la Plaignante, notamment par le biais du registre des activités de traitement (« RoPa »),
    b) la/les finalité(s) pour lesquelles elles sont exécutées,

---

[37] Google Play Console Help: https://support.google.com/googleplay/android-developer/answer/6048248?hl=fr (pièce 17 « Google Advertising ID ») consulté le 26.06.2023.

[38] Projet de recommandation relative aux applications mobiles de la CNIL, page 30, point 3.

[39] Projet de recommandation relative aux applications mobiles de la CNIL, page 30, point 3.

[40] Voir Batch « SDK integration documentation under 'Optional dependencies' » https://doc.batch.com/android/sdk-integration/#optional-dependencies (pièce 18 « Batch SDK integration ») consulté le 26.06.2023.

c) la base légale sur laquelle le responsable du traitement s'appuie pour chaque traitement spécifique, et leur validité.

61. La Plaignante demande également que les résultats de cette enquête lui soient communiqués au cours de la procédure, conformément à l'article 77(2) RGPD et à l'article 41 de la Charte des droits fondamentaux de l'UE.

7.2. Demande d'obtenir l'effacement des données à caractère personnel et d'informer les destinataires de cet effacement

62. La Plaignante demande :

a) au responsable du traitement d'effacer toutes les données à caractère personnel traitées illégalement (article 17(1)(d) RGPD)
b) qu'il soit ordonné au de cesser de divulguer les données à caractère personnel de la plaignante et d'informer tous les destinataires des données de la plaignante que celle-ci a demandé l'effacement par les destinataires de tout lien vers ses données à caractère personnel, ou de toute copie ou réplication de celles-ci (article 17(2) RGPD).

7.3. Imposition d'une amende

63. Enfin, la Plaignante suggère que l'autorité de surveillance, en vertu des pouvoirs qui lui sont conférés par l'article 58(2)(i), lu en combinaison avec l'article 83(5)(a) du RGPD, impose une amende effective, proportionnée et dissuasive à l'encontre du responsable du traitement, compte tenu des éléments suivants :

a) la gravité de l'infraction, étant donné que le traitement licite est la pierre angulaire du droit fondamental à la protection des données à caractère personnel (article 83(2)(a) du RGPD) ;
b) le responsable du traitement a délibérément et intentionnellement violé la loi en fondant ses modèles commerciaux sur l'abus des droits des consommateurs et sur le traitement de données à caractère personnel sans base juridique (article 83(2)(b) du RGPD) ;
c) une violation délibérée, massive et profonde par des acteurs majeurs de l'industrie des données doit être sanctionnée de manière adéquate afin de prévenir des violations similaires du RGPD à l'avenir et de garantir le respect des droits des consommateurs dans le cadre du nouvel *acquis en matière* de protection des données.

64. Nous demandons le prononcé d'une amende adéquate, compte tenu notamment de la gravité des violations constatées, mais également du nombre potentiellement très élevé de personnes concernées et du profit tiré par les activités de traitement illégales par les sociétés concernées.

8. CONTACT

65. Les communications entre *noyb* et l'Autorité de surveillance dans le cadre de cette procédure peuvent être effectuées par courrier électronique à l'adresse [redacted] en faisant référence à **l'affaire n° C**[redacted] et sous le numéro : [redacted].