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
By the CNIL complaints department

Vienna, 14.09.2023

noyb Case-No : [redacted]

Complainant : [redacted]

represented pursuant to Article 80(1) RGPD by : *noyb* - European Centre for Digital Rights
Goldschlagstraße 172/4/3/2, AT-1140 Vienna, Austria

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

and any other entity that the Authority deems responsible for the violations

Concerns : Infringement of Article 5(3) of the Directive on privacy and electronic communications,
Infringement of article 82 of the French Data Protection Act,
Infringement of Articles 5(1) (a), 6(1)(a) and 25(1) and (2) GDPR.

COMPLAINT

1. REPRESENTATION

1. *noyb* - European Center for Digital Rights is a non-profit organisation active in the field of the protection of the rights and freedoms of data subjects, with registered office at Goldschlagstraße 172/4/2, 1140 Vienna, Austria, ZVR registration number: 1354838270 (hereinafter: "*noyb")* (Exhibit 1 "noyb statutes").

2. *noyb* represents the Complainant pursuant to Article 80(1) of the GDPR (Exhibit 2 "Representation Agreement").

2. FACTS OF THE CASE

3. The data controller, FNAC, is a French online electronics shop. The data controller describes its mobile app (hereinafter "mobile app"; "app"): "*Entirely thought out for you and based on your feedback, the Fnac app has been designed to provide you with a simple, convenient, enjoyable and as always 100% secure shopping experience."*[1] The app essentially allows users to browse the shop and place an order.

2.1. Complainant's device and personal data

4. The complainant installed the controller's Fnac mobile application on her phone, a Samsung S9+ [redacted], on [redacted] from the Google PlayStore. She was connected to the PlayStore with her Google account [redacted].

5. The Complainant's phone runs on the Android 10 [redacted] operating system (hereinafter "OS"). The exact specifications of the OS are as follows (see Exhibit 3 "Methodology" for OS details):
   [redacted]

6. In the context of this complaint, Google Play Services has been replaced by MicroG[2] . Unlike Google Play Services, MicroG never returns the same Android advertising identifier (hereinafter "AdID"). Each time a mobile application reads it, a new AdID is generated and returned. In other words, if a given mobile application reads the AdID three times, the operating system will return three different AdIDs. The unique AdID issued for the Fnac application was: [redacted].

7. The phone was connected to the [redacted] mobile network with the phone number: [redacted]. The phone number is registered to the complainant.

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

[2] https://microg.org/

2.2. Traffic between the controller's mobile application and the tracking company

8. On [redacted] between [redacted] and [redacted] (hereinafter "the Relevant Period"), the Petitioner used the Fnac mobile application. The Relevant Period was determined by the first launch of the application and its subsequent closing (see Exhibit 3 for the complete technical documentation and methodology, and Exhibit 4 "Screen Recording" for a screen recording of the Complainant's use of the application during the Relevant Period).

9. Immediately after the first launch of the application, a banner was presented to the Complainant. A screenshot of this banner is attached as Exhibit 5 "Screenshot of Banner".

10. The complainant did not interact with the banner or the application in any way (i.e., she did not click on the phone screen) (see Exhibit 4), other than to close the application.

11. The Fnac application includes software development kits[3] (hereinafter "SDKs"), one of which belongs to the user analytics company Batch[4] (hereinafter "Tracking Company"; "Recipient") (Exhibit 6 "Exodus Report").

12. According to Exodus Privacy, Batch provides analytics and profiling services[5] . In Batch's own words: "*Batch is THE next generation customer engagement platform. We help create relationships between customers and their favourite brands through a highly personalised experience" (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. In other words, Batch offers application developers sophisticated user analytics. On the basis of these analyses, Batch enables its customers to send users of their applications personalised messages, generally for marketing purposes[7] .

14. Batch itself provides an example of how it helped Fnac generate €214,000 through a push marketing notification announcing the pre-order of the new Nintendo Switch at Fnac (see screenshot below).

---

[3] Software that can be incorporated into other software for functional or advertising purposes.

[4] See the full list provided by Exodus Privacy: https://reports.exodus-privacy.eu.org/en/reports/fr.fnac.com/latest/ consulted on 25.06.2023; Exhibit 6 "Exodus Report".

[5] As provided by Exodus Privacy: https://reports.exodus-privacy.eu.org/en/trackers/23/, consulted on 25.06.2023.

[6] Free translation; https://help.batch.com/en/articles/1622557-what-is-batch, consulted on 26.06.2023; Exhibit 7 "What is Batch".

[7] See a "non-exhaustive list" of the objectives of the Batch SDK: https://help.batch.com/en/articles/4393095-what-purpose-is-batch-sdk-serving (Exhibit 8 "What purpose is Batch SDK serving"). See also: https://batch.com/about (Exhibit 9 "Batch About"), consulted on 08.08.2023.

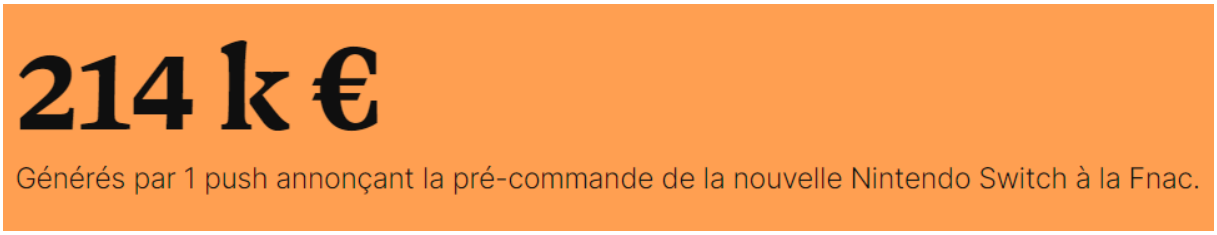


Figure 1. Batch.com: "Why Retailers go with Batch".[8] consulted on 15 June 2023.

15. Batch therefore processes personal data on behalf of the controller and is considered to be the controller's processor under Article 4(8) GDPR.

16. According to Batch's developer documentation, the Batch SDK collects users' AdID and advanced device data by default[9] . By embedding the "default" code from the specified tracking library, the Fnac app accesses its users' data through the SDK by default and shares it with the Batch tracking company for user analysis and profiling.

17. During the Relevant Period, the Petitioner observed that the Fnac application was sending multiple requests[10] (hereinafter "Traffic") containing the Complainant's personal data to servers belonging to Batch (Exhibit 12 "Colander Report").

18. The data transmitted included: the AdID, device model, device brand, operating system version and other user identifiers generated by Batch. The Fnac application transmitted the Complainant's AdID to the Batch tracking company five times per minute. Below is an example of data transmission between Fnac and Batch:

[Image redacted]

Figure 2. Example of traffic data from the Fnac application to Batch containing AdID, personalised identifiers and advanced device data, [redacted] (see Exhibit 12 "Colander Report" and Exhibit 13 "Traffic" for full details).

19. A detailed record of all traffic between the controller's application and the various servers during the period in question is attached as Exhibit 13 "Traffic".

3. APPLICABLE LAW

20. The storage of and access to personal and non-personal data on the Complainant's device is governed by Article 5(3) of Directive 2002/58/EC on privacy and electronic communications ("Directive on privacy and electronic communications").

21. The Privacy and Electronic Communications Directive is transposed in France by Article 82 *of the Data Protection Act*, which transposes Article 5(3) of the Directive.

---

[8] https://batch.com/customers/retail, (Exhibit 10 "Why Retailers Go with Batch") consulted on 08.08.2023.

[9] https://doc.batch.com/android/custom-data/advanced/#advertising-id and https://doc.batch.com/android/custom-data/advanced/#advanced-device-information (Exhibit 11 "Batch Advanced") consulted on 12.06.2023.

[10] Message sent by a client to a server containing information about a web resource and how the client wishes to interact with it.

22. In accordance with Article 5(3) of the aforementioned Directive, "[...] *the storage of information, or access to information already stored, in the terminal equipment of a subscriber or user is authorised only if the subscriber or user concerned has given his or her consent [...]*". Article 82 *of the French Data Protection Act* stipulates the following:

> *Any subscriber or user of an electronic communications service must be informed in a clear and comprehensive manner, unless they have been informed in advance by the controller or its representative:*
>
> *1°The purpose of any action to access, by electronic transmission, information already stored in his electronic communications terminal equipment, or to write information into that equipment ;*
>
> *2° The means available to the subscriber or user to oppose such access or registration. Such access or registration may only take place on condition that the subscriber or user, after having received this information, has expressed his or her consent, which may result from appropriate settings on his or her connection device or any other device under his or her control.*
>
> *These provisions shall not apply if access to information stored in the user's terminal equipment or the recording of information in the user's terminal equipment :*
>
> *1° Or, has the sole purpose of enabling or facilitating communication by electronic means;*
>
> *2° Or is strictly necessary for the provision of an online communication service at the express request of the user.*

23. The further processing of the Complainant's personal data, i.e. the transmission of personal data to third parties for the purposes of user analysis and profiling, is governed by the GDPR and must comply, inter alia, with Articles 5(1)(a), 6 and 25 of the GDPR.

4. COMPETENT AUTHORITY

24. As the data controller's principal place of business is in France[11] , the CNIL is competent to examine this complaint.

5. CONTEXT: UNCONTROLLED TRACKING IN MOBILE APPLICATIONS

25. A number of studies have reported widespread and uncontrolled tracking of mobile application users, without their knowledge and in breach of the applicable legislation[12] .

[11] See the privacy policy of the data controller: https://www.fnac.com/Help/donneesPersonnelles (Exhibit 14 "Fnac Privacy Policy").

[12] See, for example, 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 (accessed 13 April 2023); Konrad Kollnig et. al, Before and after RGPD: tracking in mobile apps: https://policyreview.info/articles/analysis/and-after-RGPD-tracking-mobile-apps (accessed 13 April 2023); Trung Tin Nguyen et. al, Share First, Ask Later (or Never?) Studying Violations of RGPD's Explicit

26. According to mnemonic[13] , a Norwegian cybersecurity company, the privacy policies of applications are relatively rarely updated, given that the third parties with which applications share data change frequently and are often even chosen dynamically, i.e. without the application provider or the data subject being aware of this in advance. Confidentiality policies therefore often do not reflect the reality of data sharing.

27. From the user's point of view, it is therefore difficult to understand with whom their data is being shared and to control it. The online advertising sector has been described as the source of the "*world's largest data breach*"[14] .

28. The prevalence of this data-sharing model is confirmed by a study conducted by Kollnig et al: 88.73% of the 12,000 Android applications studied and 79.35% of the 12,000 iOS applications sampled contained at least one tracking library.[15] The average app on both platforms contacted a similar number of tracking domains (2.7 on Android and 2.4 on iOS) before any interaction with the user. Only 18.6% of Android apps and 31.5% of iOS apps did not contact any tracking domains at app launch.[16] 55.4% of Android apps and 31% of iOS apps shared the phone's unique advertising identifier (AdID) with third parties. 85.1% of Android apps and 61.4% of iOS apps shared the phone's model and name, which often contains the phone user's first and last name.[17]

29. Other studies support this conclusion, including a study by the Institute for Application Security at the Technical University of Braunschweig, which found that almost 73% of applications sent requests containing personal data directly when the application was launched, before any other interaction with the user.[18] CMP provider UserCentrics' own research also shows that "*nine out of ten applications collect personal data from users without their consent*".[19]

30. In addition, according to further research[20] , 43.7% of the 1,297 Android apps surveyed that displayed a pop-up banner at app launch offered only one choice, such as a button labeled "Accept policy and use app" or mandatory checkboxes with no alternatives. In addition, 20.2% of applications allowed users to give or refuse their consent, but left the application

---

Consent in Android Apps: https://www.usenix.org/system/files/sec21-nguyen.pdf (accessed 13 April 2023); Benjamin Altpeter, Worrying confessions: A look at data safety labels on Android: https://www.datarequests.org/blog/android-data-safety-labels-analysis/ (accessed on 13 April 2023).

[13] Andreas Claesson and 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 (accessed on 13 April 2023).

[14] ICCL trial, 15 June 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, (accessed on 13 April 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, (accessed on 13 April 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, (accessed on 13 April 2023).

[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 (accessed 13 April 2023).

[19] Usercentrics (2022): https://usercentrics.com/press/apps-report/ (consulted on 13 April 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 (consulted on 13 April 2023).

immediately if they refused. Only 3.5% of applications offered users the option of refusing consent.[21]

31. In addition, only 3 of the 13 SDK tracking libraries evaluated include a mechanism for collecting user consent by default, and none of the five most common trackers do so (four of which belong to Google and one to Meta (formerly Facebook)).[22]

32. When informed of potential breaches of the GDPR, many app developers responded that they thought having a privacy policy in place was sufficient to presume user consent.[23]

33. While tracking companies often provide guidance to developers on RGPD compliance, this guidance can be hard to find, hard to read and poorly maintained.[24] That said, it is primarily the responsibility of app developers to ensure that they collect valid RGPD consent for storing or accessing information on the user's device and for further processing of the user's personal data for tracking purposes.

6. GROUNDS FOR COMPLAINT

6.1. Access to the Complainant's data without her consent is unlawful

34. The data controller accessed the complainant's data stored on her device when it was shared with Batch (Exhibit 13 "Traffic"), triggering the consent requirement under Article 5(3) of the ePrivacy Directive and Article 82 *of the French Data Protection Act*.

35. As explained in section 2.2 the complainant did not interact with the banner presented to her at the launch of the application, nor did she consent to access to the data on her device (Exhibit 4 "Screen recording").

36. Article 5(3) of the Directive on privacy and electronic communications and article 82 *of the French Data Protection Act* provide for specific exemptions to the consent requirement when such access is technically necessary for the transmission of a communication (Directive on privacy and electronic communications) or is "*strictly necessary*" (Directive on privacy and electronic communications and French *Data Protection Act*) for the provision of an information society service explicitly requested by the subscriber or user.

37. None of these exceptions apply in this case. The data was accessed for the purposes of user analysis and profiling, neither of which is strictly necessary to provide a functionality

[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 (consulted on 13 April 2023).

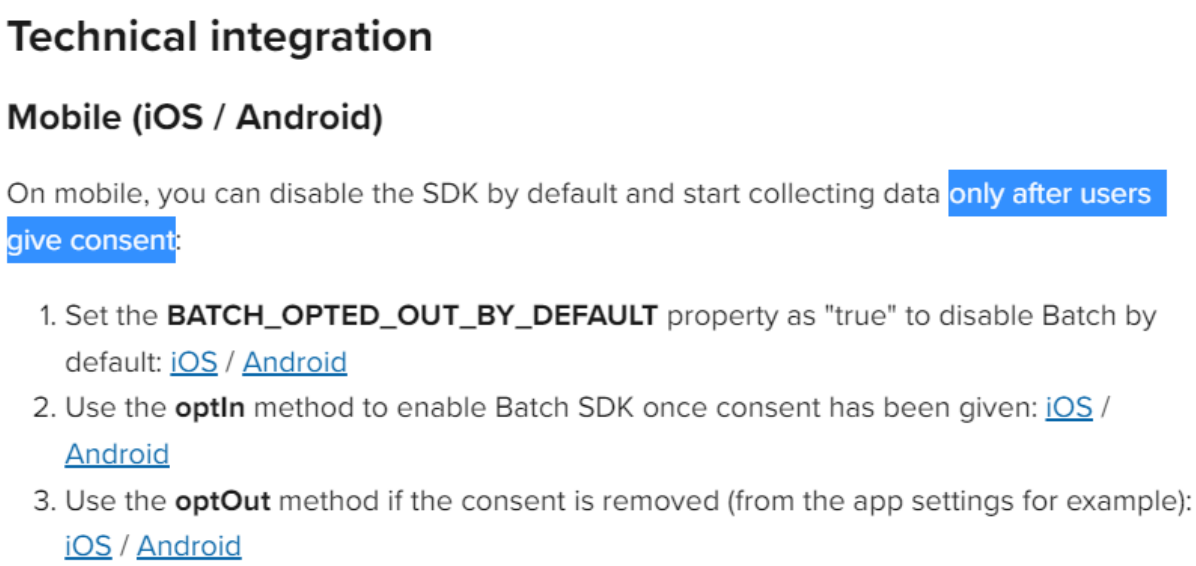
[22] Kollnig et al, A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps, 5.2, p. 9: https://arxiv.org/pdf/2106.09407.pdf (consulted on 13 April 2023).

[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 (accessed 13 April 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 (consulted on 13 April 2023).

explicitly requested by the complainant, namely the use of the application. Nor was the data consulted technically necessary for the transmission of a communication. [25]

38. Batch explains how to integrate the SDK so that data is only collected with the user's consent. However, this is not the case here.[26]



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. Batch SDK guide to integrating Batch into the CMP (12 June 2023).

39. The data controller therefore breached Article 5(3) of the ePrivacy Directive and Article 82 of *the French Data Protection Act* by accessing the information contained in the Complainant's device without her consent.

6.2. Further processing of the Complainant's data without her consent is also unlawful.

40. The data controller has shared the AdID, the model of the device, the brand of the device and the version of the operating system. The AdID is an "*advertising identifier is a unique identifier, resettable by the user, for advertising*"[27] provided by the operating system. The AdID therefore makes it possible to display targeted advertising to the user. Therefore, given that the AdID is 1) unique, 2) associated with the user (either by itself or by aggregation with other data, such as device model, device brand, operating system version, other unique user identifiers), and that it allows the user to be identified, it is considered personal data within the meaning of Article 4(1) GDPR.

41. Even in scenarios where the operating system successively generates several identifiers each time the application requests access to the AdID, any AdID processed by the SDK provider remains personal data because it is associated with the user. Generating and transmitting

[25] See the CNIL's draft recommendations on mobile applications, pages 28-29.

[26] https://help.batch.com/en/articles/5204072-how-to-integrate-batch-into-my-cmp (exhibit 15 "How to integrate Batch into my CMP") consulted on 12.06.2023. Note that Batch explains how to integrate the SDK so that data is only collected with the user's consent. However, this is not the case here.

[27] Google Play Console Help: https://support.google.com/googleplay/android-developer/answer/6048248?hl=fr (Exhibit 17 "Google Advertising ID") consulted on 26.06.2023.

several AdIDs does not break the association between the user and the AdID. Furthermore, AdIDs are rarely transmitted to the SDK provider in isolation. They are generally transmitted with other data that remains unchanged. Finally, the SDK provider specifically seeks to link the different devices and profiles (as an AdID may be called) of users[28] .

42. The data controller collected the Complainant's personal data and transmitted it to the tracking company Batch for the purposes of user analytics and profiling. This amounts to "processing" within the meaning of Article 4(2) GDPR.

43. In accordance with Article 5(1)(a) of the RGPD, processing must be lawful, fair and transparent. To comply with the lawfulness principle, the data controller must rely on one of the six legal bases set out in Article 6 of the RGPD.

6.2.1. The data was processed without the Complainant's consent, which is the only relevant legal basis in this case.

44. As explained in the Batch documentation and website, Batch is a customer engagement platform that provides application developers with sophisticated user analytics, including profiling, as well as personalised messaging capabilities, typically for marketing purposes, to the users of those applications based on the user analytics performed. [29]

45. Fnac, as data controller, must ensure that this processing carried out by Batch on behalf of Fnac is lawful. This extensive processing is considered high-risk data processing and should only be carried out after obtaining valid consent under the GDPR (Article 6(1)(a) of the GDPR)[30] .

46. If a data controller relies on consent as the legal basis for accessing personal data, it must rely on the same legal basis for any downstream processing carried out for the same purpose. Any other solution would be tantamount to circumventing the protection that the ePrivacy Directive seeks to provide by requiring prior consent.

47. This point of view is supported by the EDPB and the EDPS, which jointly recall:

"[...] *that where consent is required under Article 5(3) of the ePrivacy Directive, consent under Article 6 of the GDPR would most likely be the appropriate legal basis for any processing of personal data subsequent to storing information or obtaining access to information already stored in the terminal equipment of a subscriber or user".*[31]

---

[28] See for example https://help.batch.com/en/articles/6441020-how-to-fill-out-the-advertising-id-collection-form-in-the-play-console (Exhibit 20 "Batch Knowledge base") consulted on 21.08.2023.

[29] See a "non-exhaustive list" of the objectives of the Batch SDK: https://help.batch.com/en/articles/4393095-what-purpose-is-batch-sdk-serving (Exhibit 8 "What purpose is Batch SDK serving"). See also: https://batch.com/about (Exhibit 9 "Batch About"), consulted on 08.08.2023.

[30] See for example page 32 of WP29 Opinion 06/2014 on the notion of legitimate interests (06/2014) and page 46 of WP29 Opinion 03/2013 on purpose limitation (03/2013), which state that profiling and analysis require the consent of the data subject.

[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), paragraph 44.

48. However, in this case, as already developed in section 6.2 above, and as confirmed by the CNIL in its draft recommendation on mobile applications[32] , Fnac must therefore ask users for valid consent under the GDPR to process their personal data for the purposes of analysing and profiling the user via Batch.

49. In particular, Batch itself recommends that the data controller should rely on consent to process user data.[33]

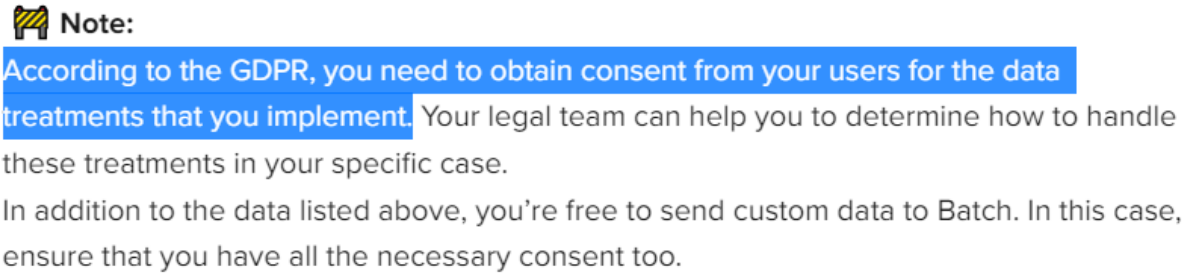


Figure 4. Batch SDK guide "GDPR Compliance" (Exhibit 16 "Batch GDPR Compliance") consulted on 11 June 2023.

50. The data controller acts as a "first party" vis-à-vis the Complainant. This means that the Complainant interacts directly with the data controller when using its application. As a result, the data controller is also responsible for ensuring that it obtains valid consent from the Complainant within the meaning of the GDPR to share her personal data with third parties whose SDKs it integrates into the mobile app.[34]

51. The Complainant did not give her consent (see section 2.2). In any event, in accordance with Article 7(1) of the GDPR, the data controller must demonstrate that the Complainant has consented to the processing of her personal data.

6.3. The principles of data protection by default and by design (Article 25 of the RGPD)

52. As reiterated by the CNIL in its draft recommendation[35] , the application publisher must apply data protection principles by default and from the design stage, in accordance with Article 25 of the RGPD.

53. Batch's developer documentation shows that the Batch SDK collects AdID and advanced device data by default despite the fact that this collection requires prior consent. [36] Batch could

[32] CNIL draft recommendation on mobile applications, page 28-29.

[33] See also: https://help.batch.com/en/articles/1957231-gdpr-compliance, (Exhibit 16 "Batch GDPR Compliance") consulted on 11.06.2023.

[34] See Deliberation SAN-2023-009 of 15 June 2023 concerning CRITEO and the press release on https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million, consulted on 03.07.2023.

[35] CNIL draft recommendation on mobile applications, 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, consulted on 26.06.2023 (Exhibit 11 "Batch Advanced").

have made its code compliant with legal requirements by only allowing AdID collection on the condition that prior consent was given. However, Batch decided to write its code in breach of the requirements of the ePrivacy Directive and the GDPR.

54. It is clear, however, that FNAC did not change the default code in the Batch SDK by integrating the code into the application, since data collection began as soon as the Complainant launched the application.

55. In addition, FNAC processed the Complainant's AdID for analytical purposes (see section 2.2). However, such processing is not necessary for the provision of the service. The AdID, according to Google's documentation, is "a unique identifier that can be reset by the user and is used for advertising. It gives users more control and provides a simple, standardised system for developers who want to continue monetising their applications.[37] Clearly, the purpose of the AdID is to enable developers to monetise their applications for advertising purposes.

56. As the CNIL points out in its draft recommendation on mobile applications, providing for processing that is not essential to the provision of the service contravenes the principles of data protection by default and by design. [38]

57. In addition, the publisher should allow the end user to choose whether or not to use features that are not strictly necessary for the application to function properly. [39]

58. As already mentioned, the Batch SDK collects the data by default, but collection of the AdID is optional and can be disabled by the application developer, according to Batch. [40]

59. By not deactivating the default collection and processing of the AdID for Analytics purposes, and therefore allowing unnecessary collection of data, FNAC therefore breached the principle of data protection by default and by design.

7. REQUESTS

7.1. Request for investigation

60. The Complainant requests your Authority to conduct a thorough investigation of this complaint, in accordance with Article 58(1) a), e) and f), of the GDPR, in order to determine, inter alia

    a) the processing operations carried out by the data controller with regard to the Complainant's personal data, in particular through the register of processing activities ("RoPa"),

[37] Google Play Console Help: https://support.google.com/googleplay/android-developer/answer/6048248?hl=fr (Exhibit 17 "Google Advertising ID") consulted on 26.06.2023.

[38] CNIL draft recommendation on mobile applications, page 30, point 3.

[39] CNIL draft recommendation on mobile applications, page 30, point 3.

[40] See Batch "SDK integration documentation under 'Optional dependencies'" https://doc.batch.com/android/sdk-integration/#optional-dependencies (part 18 "Batch SDK integration") consulted on 26.06.2023.

b) the purpose(s) for which they are carried out,
c) the legal basis on which the data controller relies for each specific processing operation, and their validity.

61. The Complainant also requests that the results of this investigation be communicated to it during the proceedings, in accordance with Article 77(2) GDPR and Article 41 of the EU Charter of Fundamental Rights.

7.2. Request for the deletion of personal data and to inform the recipients of such deletion

62. The Complainant requests :

a) the controller to erase all personal data processed unlawfully (Article 17(1)(d) GDPR)
b) that the complainant be ordered to cease disclosing her personal data and to inform all recipients of her data that she has requested the recipients to erase any links to, copies of or replications of her personal data (Article 17(2) GDPR).

7.3. Imposition of a fine

63. Finally, the Complainant suggests that the supervisory authority, by virtue of the powers conferred on it by Article 58(2)(i), read in conjunction with Article 83(5)(a) of the GDPR, impose an effective, proportionate and dissuasive fine on the controller, taking into account the following:

a) the seriousness of the offence, given that lawful processing is the cornerstone of the fundamental right to protection of personal data (Article 83(2)(a) of the RGPD);
b) the controller has deliberately and intentionally breached the law by basing its business models on the abuse of consumer rights and the processing of personal data without a legal basis (Article 83(2)(b) of the GDPR) ;
c) a deliberate, massive and far-reaching breach by major players in the data industry must be adequately sanctioned in order to prevent similar breaches of the GDPR in the future and to ensure that consumers' rights are respected under the new data protection *acquis.*

64. We are calling for an appropriate fine to be imposed, particularly in view of the seriousness of the breaches observed, but also in view of the potentially very large number of people affected and the profit made by the companies concerned from their illegal processing activities.

8. CONTACT

65. Communications between *noyb* and the Supervisory Authority in connection with these proceedings may be made by e-mail to [redacted] with reference **to case no.** [redacted] and under the number: [redacted].