Decision no. 2016-007 of January 26, 2016 issuing formal notice to FACEBOOK INC. and FACEBOOK IRELAND

The Chair of the *Commission Nationale de l'Informatique et des Libertés* (French data protection authority),

Pursuant to Convention no.108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Pursuant to European Parliament and Council Directive 95/46/EC of October 24, 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data;

Pursuant to the French Penal Code;

Pursuant to Act 78-17 of January 6, 1978 (French Data Protection Act), as amended, and in particular Article 45;

Pursuant to Decree no. 2005-1309 of October 20, 2005, as amended, in accordance with Act no. 78-17 of January 6, 1978 (French Data Protection Act);

Pursuant to decision no. 2013-175 of July 4, 2013 pertaining to the adoption of the by-laws of the *Commission Nationale de l'Informatique et des Libertés*;

Pursuant to the rulings handed down by the Court of Justice of the European Union on May 13, 2014 in case C-131/12 Google Spain SL and Google Inc. versus *Agencia Española de Protección de Datos* (AEPD) and Mario Costeja González, on October 1, 2015 in case C-230/14 Weltimmo s.r.o. versus *Nemzeti Adatvédelmi és Információszabadság Hatóság* and on October 6, 2015 in case C-362/14 Maximillian Schrems versus Data Protection Commissioner;

Pursuant to the decisions of the Chair of the *Commission Nationale de l'Informatique et des Libertés* to verify the processing of personal data by FACEBOOK Inc. (no. 2015-091C of March 17, 2015) and pertaining, in whole or in part, to data collected through the website FACEBOOK.COM or through cookies associated with this domain (no. 2015-401C of December 14, 2015);

Pursuant to on-site inspection reports no. 2015-091/1 and no. 2015-091/2 of April 8 and 9, 2015, the answers provided by FACEBOOK INC. to the questionnaire sent by CNIL on July 30, 2015 and the report of online inspection no. 2015-401 of December 15, 2015;

Pursuant to the other documents in this case;

I- Notes the following

FACEBOOK Inc. was founded in 2004 and its head office is in the United States (1601 Willow Road, Menlo Park, CA 94025). Its business is to manage the FACEBOOK social network (FACEBOOK.COM) (hereinafter referred to as the "website") and it has approximately 1.5 billion active users per month around the world. The company also has an advertising management activity. It has 49 offices in some thirty countries, with approximately 12,000 employees internationally.

FACEBOOK Inc. has founded dozens of subsidiaries around the world, including FACEBOOK Ireland Limited, based at 4 Grand Canal Square, Grand Canal Harbour, Dublin, and FACEBOOK France Sarl, based at 108 Avenue de Wagram in Paris (75017).

In accordance with decision no. 2015-091C of March 17, 2015 of the Chair of the *Commission Nationale de l'Informatique des des Libertés* (hereinafter referred to as "CNIL" or "the Commission"), a CNIL delegation performed an on-site inspection on April 8 and 9, 2015 and a documentary audit on July 30, 2015. With decision no. 2015-401C of December 14, 2015 of the Chair of the CNIL, an online inspection has also been performed on December 15, 2015. The purpose of these operations was to verify that FACEBOOK Inc. was acting in compliance with the provisions of French Act no.78-17 of January 6, 1978, as amended, with regard to confidentiality regulations applicable to services aimed at French Internet users. They also focused on data collected via FACEBOOK.COM and cookies associated with this domain.

The applicability of the French law

It is first stated that, as per Article 4 thereof, Directive 95/46/EC applies when "*the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*". Article 5 of the French Act of January 6, 1978, as amended, states that French law applies if the controller is established on French territory.

French law is applicable because FACEBOOK France is an "establishment" within the meaning of Directive 95/46/EC, according to the interpretation of the Court of Justice of the European Union (CJEU) in its Weltimmo ruling of October 1, 2015. In addition, the data processing implemented within the framework of the FACEBOOK social network is carried out "*in the context of the activities*" of this establishment within the meaning of the CJEU Costeja ruling of May 13, 2014.

Furthermore, in light of the findings and documents supplied during the various inspections, both FACEBOOK Inc. and FACEBOOK Ireland (hereinafter the "company") contribute to determining the purpose and means of processing. Both companies must therefore be considered jointly responsible for processing, as allowed by Directive 95/46/EC. Indeed, article 2(d) of said directive defines the "*controller*" as "*the natural or legal person, public*

authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."

The fact that one of the data controllers, FACEBOOK Ireland, is located within the European Union makes no difference in terms of inspections or sanctions. Article 48 of the aforementioned Act states that CNIL may exercise these powers "*as regards any processing operations carried out, whether fully or partially, on the national territory, including where the data controller is established in another Member State of the European Union.*"

The facts

The delegation was informed that the company collects data concerning the browsing activity of Internet users on third-party sites who do not have a FACEBOOK.COM account.

The delegation was also informed that the company sends some personal data belonging to Internet users to the United States via the Safe Harbor principles.

It observed that the company collects data concerning the sexual orientation, religious views and political opinions of its account holders. The company sometimes also collects medical records provided by account holders as proof of identification.

Furthermore, the delegation was informed that the company compiles large amounts of data about account holders without a legal basis for doing so, and that it has implemented data processing without the authorization of CNIL for the purpose of combatting fraud and banning account holders from its website.

It also observed that the sign up form for the website contains no information concerning the processing of personal data and that no information is given to Internet users, in particular, concerning the purpose of sending data to the United States.

Furthermore, the delegation observed that 13 cookies were placed on its terminal.

The delegation also observed that the company stores all IP addresses used by account holders to connect to their accounts.

Finally, the delegation observed that Internet users who wish to create an account on the website can choose a 6-character password.

II- Regarding the failures to comply with the provision of the French Act of January 6, 1978, as amended

Failure to comply with the obligation to have a legal basis for data processing

The delegation was informed that the company compiles various information items for the purposes of displaying targeted advertising to account holders and measuring the effectiveness of advertising campaigns. The company's Data Policy states that "*We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services.*"

The hyperlink "*Information we have*" returns the user to the top of the Data Policy, where the first section lists the kinds of information collected by the company. In response to the questionnaire, the company confirmed that it could use all this data for delivering targeted advertising (answer to question 11).

The company therefore particularly compiles the following information:

- information provided by account holders when creating their account;
- information concerning the activity of account holders on the website (e.g. content shared or viewed), regardless of the device they use;
- information concerning devices (computer, telephone, etc.) used by account holders (e.g. Operating System, GPS coordinates, browser type, mobile telephone number.);
- information from third-party websites and applications which use the "*Like*" and "*Facebook Log In*" buttons (e.g. websites viewed and applications used);
- information from third-party partners (partners with whom the company works to jointly offer services or advertisers with whom account holders have interacted) (e.g. e-mail address);
- information from companies owned or operated by the company (e.g. Facebook Payments Inc., Instagram LLC, WhatsApp Inc.)

However, the personal data of account holders may only be compiled like this for advertising purposes if the company can claim one of the conditions set out in Article 7 of French Act no.78-17 of January 6, 1978, as amended, which states that: "*processing of personal data must have received the consent of the data subject or must meet one of the following conditions:*

1° compliance with any legal obligation to which the data controller is subject;

2° the protection of the data subject's life;

3° the performance of a public service mission entrusted to the data controller or the data recipient;

4° the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract;

5° the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject."

In the case at hand, because account holders have not given their prior consent before their data is compiled, only one of the conditions listed 1 to 5 in the aforementioned article may constitute a legal basis for this data processing.

Given the nature of processing involved, points 1°, 2° and 3° of Article 7 cannot constitute the legal basis for the company to compile data. The processing involved in compiling this data can therefore only be considered in relation to points 4° and 5° of Article 7.

With regard to point 4° of Article 7, in the case at hand, there is no contractual framework governing data compilation for the purposes of displaying targeted advertising. Although the company mentions it in its Data Policy, compiling data does not constitute the primary object of the contract entered into by Internet users when they sign up to the website. The opportunity that the company gives itself for compiling data must be considered accessory to said contract, decided unilaterally by the company.

In this regard, it should be noted that account holders have the opportunity to refuse the display of targeted advertising in their account settings ("*Ads*" section). The ability to display targeted advertising is a direct result of data compilation. Account holders can therefore request that this function not be applied to them, which confirms that the data compilation is neither the object, nor an essential provision of the agreement.

Therefore, the company cannot base data compilation for advertising purposes on the performance of the Data Policy, such that point 4° of the aforementioned Article 7 cannot be applied to the case at hand.

With regard to point 5° of Article 7, on the one hand, the data controller's legitimate interest must be understood as it is and, on the other hand, in terms of the interest of the data subject and his/her fundamental rights and liberties, which the legitimate interest of the data controller must not infringe.

On the one hand, to understand the legitimacy of the data controller's interest, the proportionality of data processing with regard to its purposes needs to be taken into account. In the case at hand, the company states that compiling all data enables it to "*improve [its] advertising and measurement systems*".

On the other hand, it has to be noted that such data compilation is, by its very nature, scale and bulk approach, likely to be incompatible with the interests and fundamental privacy rights of account holders.

The financial and commercial interest of the company may only be considered legitimate if the data controller provides account holders with sufficient means to control how their data is compiled and effectively exercise their right recognized by Article 38 of the French Act of January 6, 1978, as amended.

As it is, the company provides no tools for account holders to prevent their personal data from being compiled, and thereby enforce their private interest or rights and liberties against the interests of the data controller. In the account settings, under "*Ads*", the company only provides account holders with tools for blocking targeted advertising:

- for ads based on account holder preferences: the company states that "*We want to show you ads that you'll find relevant. That's why we have ad preferences, a tool that lets you view, add and remove preferences that we have created for you based on things such as your profile information, actions that you take on Facebook and websites and apps that you use off Facebook (...) If you remove all of your preferences, you'll still see ads, but they may be less relevant to you.*" Account holders can remove the preferences identified by the company, but this tool does not allow them to refuse the collection and compilation of this data for advertising purposes;
- for adverts based on account holder use of websites and apps: the company states that "*one of the ways in which we show you ads is based on your use of websites and apps that use Facebook's technologies. For example, if you visit travel websites, you might then see adverts on Facebook for hotel deals.(...) If you turn off online interest-based ads you'll still see the same number of ads, but they may be less relevant to you.*" This tool does not enable account holders to exercise their right to refuse the collection and compilation of their data for advertising purposes.

The foregoing demonstrates that the compilation of all account holder data has no legal basis for lack of a sufficient contractual framework, or, in seeking its own legitimate interests as the process controller, respect for the interests and rights and freedoms of individuals, by providing them with the means to control the compilation of data concerning them and exercise their rights in an effective manner.

These facts constitute a violation of Article 7 of the French Act of January 6, 1978, as amended.

Failure to comply with the obligation to ensure the adequacy, relevance and non-excessive nature of data collected

The delegation observed that the company sometimes asks Internet users who have accounts on its website (hereinafter referd to as "account holders") to provide proof of identity, such as a medical record, for example if they try to replace their surname with that of a celebrity. On the website's Help pages, the company encourages Internet users, when they provide such

documents, to "*cover up any personal information we don't need to verify your identity (ex: credit card number, Social Security number)*".

Despite the fact that the company draws the attention of account holders to the need to cover up this information, asking for the medical records of account holders to prove their identity does not seem relevant. This kind of document includes various information items that could infringe the privacy of the individuals in question, and many other documents could be used by account holders to prove their identity.

These facts constitute a violation of Article 6-3 of the French Act of January 6, 1978, as amended, which states that data collected must be "*adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing.*"

Failure to comply with the obligation to obtain the consent of data subjects for the processing of sensitive data concerning political or religious views and sexual lifestyle

The delegation observed that once Internet users have signed up to the website they can complete their profile on the "*About*" page, under the "*Contact and basic info*" section. They can, in particular, specify their sexual orientation ("*Add who you're interested in*": "*Interested in* □ *Women* □ *Men*"), their religious views ("*Add your religious views*") and their political views ("*Add your political views*").

However, the delegation noted that the company has not included a box to be ticked so that individuals can consent to the collection of this information.

Article 8 of the French Act of January 6, 1978, as amended, states in particular that the collection or processing of personal data concerning the political or religious views or sexual lifestyle of individuals, except in the cases set out in Section II of this Article, and in particular in the event of the explicit consent of the subjects is prohibited.

However, consent can only be considered explicit if it is given with full knowledge of the situation, i.e. after providing sufficient information on how personal data will be used.

In the case at hand, no technical means are made available to individuals when "sensitive" data is collected and processed in order to ensure that they give their explicit consent on the basis of specific information.

CNIL considers that the fact that individuals in question enter their sensitive data may not be deemed explicit consent. Users must be able to indicate their assent by ticking a box to authorize the use of their sensitive personal information, which is not currently the case.

These facts constitute a violation of Article 8 of the French Act of January 6, 1978, as amended.

Finally, it is hereby stated that in accordance with Articles 226-19 and 226-24 of the French Penal Code combined, the fact that a legal person records or preserves in a computerized memory, without the explicit consent of the person concerned, personal data which directly or indirectly reveals, the racial and ethnic backgrounds, the political, philosophical, religious views or labor union affiliation of individuals, or which concern their health or sexual orientation, is punishable by a fine of up to €1,500,000.

Failure to comply with the obligation to inform individuals

The delegation observed that the website sign up form contains no information concerning the processing of personal data.

However, Article 32 of French Act no.78-17 of January 6, 1978, as amended, imposes to provide the data subject, directly on the data collection form, with information on the identity of the data collector, the purposes of processing, whether replies to the questions are mandatory or optional, their rights to access their data, rectify it or, if applicable, object to its processing.

Furthermore, the delegation observed that the company's Data Policy states that "*Information collected within the European Economic Area ("EEA") may, for example, be transferred to countries outside of the EEA for the purposes as described in this policy.*" For Internet Users outside the United States, Article 16 of the Statement of Rights and Responsibilities states: "*You consent to having your personal data transferred to and processed in the United States.*"

However, the delegation observed that Internet users are not informed of the nature of data transferred, the purpose of the transfer, the kinds of data recipients, and the level of protection provided by third countries, which is not compliant with Article 91 of Decree of October 20, 2005, as amended, adopted pursuant to Act no.78-17 of January 6, 1978, as amended.

Indeed, this article states that "*The information referred to under Article 32 (I) (7) of the aforementioned Act of 6 January 1978 that the data controller sends, according to the conditions set out under Article 90, to the data subject from whom the personal data are collected are the following:*

1° the country or countries of establishment of the recipient of the data whenever this or these countries are indicated at the time of the collection of data;
2° the nature of the transferred data;
3° the purpose of the planned transfer;
4° the category or categories of recipients of data;
5° the level of protection offered by third countries:
a) If the third country or countries is/are on the list referred to under Article 108, the decision of the European Commission authorizing this transfer must be mentioned;

b) *If the third country or countries does/do not satisfy the conditions set out under Article 68 of the same Act, the exception referred to under Article 69 of this Act which allows this transfer or of the decision of the CNIL authorizing this transfer must be mentioned."*

These facts constitute a violation of Article 32 of French Act no.78-17 of January 6, 1978, as amended, with regard to the duty of the data collector to provide the data subject, directly on the data collection form, with information on the identity of the data collector, the purposes of processing, whether replies to the questions are mandatory or optional, their rights to access their data, rectify it or, if applicable, object to its processing.

It is hereby stated that in accordance with Articles 131-41 and R. 625-10 of the French penal code combined, the fact that a legal person that controls data does not inform the individual from whom personal data is collected, in compliance with the conditions set out in Article 32 of the French Act of January 6, 1978, as amended, is punishable by a fine of up to €7,500.

On the obligation to fairly collect and process data

While visiting a third party website offering FACEBOOK plug-ins (e.g. Like button), the delegation observed that the company collects data concerning the browsing activity of Internet users who do not have a FACEBOOK.COM account.

To this end, the company "*sets a cookie (the datr cookie) on the browser of an internet user when that person interacts directly with the Facebook website in a first-party capacity (by visiting a page on facebook.com or interacting with the facebook.com domain).*" (answer to question 18). The delegation observed that the company places the "datr" cookie on the terminal of any Internet user who visits any FACEBOOK.COM page, even if they do not have an account.

The delegation observed that the company can collect data concerning the browsing activity of Internet users who do not have a FACEBOOK account when visited third-party websites offer FACEBOOK plug-ins. Indeed, when an Internet user who do not have a FACEBOOK account visits a FACEBOOK page, then visits a third-party website offering a FACEBOOK plug-in, the information relating to the said website is transmitted to the company along with the "*datr*" cookie. The delegation was informed that "*in relation to non-account holders, access logs relating to cookies and social plug-ins are deleted within ten days*" (answer to question 27).

In this regard, the company stated that it "*does not, and has not, used the datr cookie to monitor the surfing behaviour of non-account holders for advertising purposes or otherwise. Rather, this cookie is used for essential security and integrity purposes*"" and it serves to "*(i) distinguish between authorised access requests and unauthorised access requests; (ii) prevent unauthorised access; and (iii) understand the volume and frequency of access requests in*

order to stop people or machines from scraping data, carrying out denial-of service attacks, or mass-creating fake accounts" (answer to question 18).

While the purpose claimed by the company may seem legitimate (ensuring the security of its services), collecting data on browsing activity by non-account FACEBOOK holders on third-party websites is carried out without their knowledge that. Indeed, it allows the company to know a large part of the last 10 days browsing activity of non-account holders, without them being informed, even though they only visited the FACEBOOK website once.

The abovementioned facts therefore constitute a breach of paragraph 1° of Article 6 of Law No. 78-17 of January 6, 1978, which states that personal data *"are collected and processed in a fair and lawful manner"*.

Failure to comply with the obligation to obtain prior consent from data subjects before placing information (cookies) on their electronic connection terminal device or accessing said information

Article 32-II of the French Act of January 6, 1978, as amended, states that "*Any subscriber or user of an electronic communication service shall be informed in a clear and comprehensive manner by the data controller or its representative, except if already previously informed, regarding:*

- *the purpose of any action intended to provide access, by means of electronic transmission, to information previously stored in their electronic connection terminal device, or to record data in this device;*
- *the means available to them to object to such action.*

Such access or recording may only be carried out provided that the subscriber or user has explicitly expressed, after receiving said information, their agreement that may result from appropriate parameter settings in their connection device or any other system under their control.

These provisions shall not apply if the access to data stored in the terminal device of the user or the recording of information in the terminal device of the user is:

- *either exclusively intended to enable or facilitate communication by electronic means; or*
- *strictly necessary for the provision of an online communication service at the user's express request"*.

Cookies requiring prior information and consent of Internet users are, in particular, cookies associated with targeted advertising, some audience measurement cookies and social network tracking cookies generated by "social network sharing buttons".

In order to provide professionals in the sector with guidelines, CNIL adopted Decision no. 2013-378 of December 5, 2013, pertaining to the adoption of a recommendation concerning cookies and other tracking technologies. This recommendation, which does not have an

imperative nature, seeks to interpret the aforementioned legislative provisions and inform players about the implementation of specific measures for ensuring compliance with these provisions so that they either implement these measures or measures with an equivalent impact.

The recommendation states that "*the validity of consent is associated with the quality of information received.*" CNIL therefore recommends that consent be obtained in two stages:

- first stage: "*Internet users who go to a website (whether to the homepage or a secondary page) must be informed, through the display of a banner: of the specific purposes of the Cookies used; of the option to block these Cookies and change the settings by clicking a link in the banner; of the fact that continuing to browse is deemed consent to the use of Cookies on their terminal*";
- second stage: "*individuals must be informed in a simple and understandable way of the solutions provided for accepting or blocking some or all of the cookies requiring consent: for all technologies covered by Article 32-II mentioned above; by purpose category: in particular advertising, social network buttons and audience measurement*".

In addition, the recommendation states that consent "*must be expressed through a positive action by individuals who have received prior information on the consequences of their choice and have the means to exercise it*" and that it "*may only be deemed valid if the individuals in question are able to exercise their choice in a valid way and are not exposed to significant negative consequences if they refuse to give their consent.*"

In the case at hand, the delegation observed that 13 cookies were placed on its terminal device while visiting "facebook.com". Asked about the purposes of these cookies, the company referred the CNIL to its Cookie use policy and to the reports of audits by the Data Protection Commissioner (Ireland) dated 2011 and 2012.

Furthermore, the website Cookie Use policy ("*Cookies, Pixels and Similar Technologies*") states that "*things like Cookies and similar technologies (...) are used to understand and deliver ads, make them more relevant to you, and analyze products and services and the use of those products and services*". In addition, the 2012 audit report by the Data Protection Commissioner stated that the "fr" cookie, which is placed by the ".facebook.com" domain, has an advertising purpose.

However, cookies that have an advertising purpose cannot be used without prior information and consent of the individuals concerned.

In this regard, the delegation observed that Internet users are informed that "*Cookies help us provide, protect and improve Facebook's services. By continuing to use our site, you agree to our cookie policy* ».

Therefore, Internet users are not informed:

- of the purpose of all the cookies that require consent (in particular for advertising);
- of the option to change cookie settings by clicking on the link in the banner.

Furthermore, the delegation observed that the Cookie Use policy to which the banner redirects states that "*Your browser or device may offer settings related to these technologies. For more information about whether these settings are available, what they do, and how they work, visit your browser or device's help material.*"

However, web browser settings may only be considered a valid mechanism for blocking cookies in two cases:

- where the website does not place technical cookies that are essential to its operation: in this case, users can set their browser to block all cookies, whether they come from the website (first-party cookies) or a third-party site (third-party cookies), including those requiring their consent, without exposing themselves to significant negative consequences;
- where the website does not use first-party cookies requiring the consent of the person concerned: in this case, users can set their browsers to block third-party cookies without preventing the website from working or running the risk of first-party cookies requiring consent being used.

In the case at hand, the website places technical cookies that are essential to its operation and first-party cookies which require the consent of the person concerned. The Cookie Use policy states that the company places authentification cookies which make it possible to know when Internet users are logged in to the website (technical cookies). The ".facebook.com" domain also places the "fr" cookie, which has an advertising purpose (first-party cookie) requiring consent).

Therefore, in the case at hand, web browser settings may not be considered a valid mechanism for blocking cookies.

In light of the foregoing, the website has not properly informed the individuals concerned and has not received their valid consent before placing cookies.

These facts constitute a violation of the aforementioned Article 32-II of the French Act of January 6, 1978, as amended, which requires prior information and consent from the data subjects before placing information (cookies) on their electronic connection terminal devices or accessing said information

Furthermore, it is hereby stated that in accordance with Articles 131-41 and R. 625-10 of the French penal code combined, the fact that a legal person that controls data does not inform data subjects and obtain their consent before accessing or placing information on their electronic connected terminal device is punishable by a fine of up to €7,500.

Failure to comply with the obligation to define and observe a retention period proportional to the purposes of the processing

The delegation observed that the company offers account holders a "*Download your Information*" tool, which enables them to receive "*a copy of [their] Facebook data*". The delegation observed, in particular, that the "*Security*" tab of this archive lists the various IP addresses used by account holders to log in to their accounts since April 9, 2015, the date at which the delegation opened a FACEBOOK.COM account.

While the need to prevent account fraud may justify the retention of this data, it does not seem proportional to retain it for more than 6 months.

These facts constitute a violation of the provisions of Article 6-5° of the French Act of January 6, 1978, as amended, which states that data "(...) *shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.*"

Furthermore, it is hereby stated that in accordance with Articles 226-20 and 226-24 of the French penal code combined, the fact that a legal person retains personal data beyond the length of time specified by statute or by regulation, by the request for authorization or opinion, or in the preliminary declaration sent to CNIL, is punishable by a fine of up to €1,500,000.

Failure to comply with the obligation to ensure data security

The delegation observed that Internet users wishing to sign up to the website are invited to select a password containing "*at least 6 characters long*", which is "*complex*" and "*hard for someone else to figure out*". Furthermore, it observed that the password "*1234567a*" was accepted.

However, a password with six characters, or one that only includes 2 complexity requirements (numbers and letters) cannot guarantee the security and confidentiality of the data to which it gives access.

These facts constitute a violation of Article 34 of French Act no.78-17 of January 6, 1978, as amended, which states that "*The data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties.*"

Furthermore, it is hereby stated that in accordance with Articles 226-17 and 226-24 of the French penal code combined, the fact that a legal person processes personal data or has it

processed without implementing the measures required by Article 34 of the aforementioned Act no. 78-17 of January 6, 1978 is punishable in particular by a fine of up to €1,500,000.

Failure to comply with the obligation to complete formalities prior to implementing processing for banning users or combatting fraud

The delegation was informed that the company had implemented processing to combat fraud. The website Data Policy states that "*We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm. For example, we may provide information to third-party partners about the reliability of your account to prevent fraud and abuse on and off of our Services.*"

In addition, the delegation was informed that the company reserves the right to ban account holders in the event of non-compliance with the Statement of Rights and Responsibilities. Article 14 of this document states that "*If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you.*"

However, the delegation observed that the company has made no authorization request for this processing.

These facts constitute a violation of the provisions of point 4° of Article 25-I of the French Act of January 6, 1978 as amended, which states that, CNIL authorization is required for "*automatic processing which may, due to its nature, importance or purposes, exclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provisions*".

It is hereby stated that in accordance with Article 226-16 paragraph 1 and Article 226-24 of the French penal code combined, the fact that a legal person, including by negligence, processes or causes data to be processed where the data concerned is of a personal nature, without respecting the formalities required by statute prior to the processing of such data is punishable by a fine of up to €1,500,000, even where committed through negligence.

Failure to comply with the obligation to have a legal basis for transferring personal data outside the European Union

Article 16 of the Statement of Rights and Responsibilities states that data concerning Internet users outside the United States is "*transferred to and processed in the United States*".

In this regard, the website Data Policy states that "*Facebook, Inc. complies with the US-EU and US-Swiss Safe Harbor framework for the collection, use and retention of information*

from the European Union and Switzerland, as set out by the US Department of Commerce." The company added that "*The European Commission approved Standard Contractual Clauses and the Safe Harbor program (in the case of US based importers) are amongst the means by which Facebook Ireland ensures such exports are (i) lawful; and (ii) adequately protect the relevant data subjects"* (response to question 10).

However, in its ruling of October 6, 2015, the Court of Justice of the European Union declared European Commission Decision no. 2000-520 of July 26, 2000 invalid. The decision concerned the adequacy of protection provided by the Safe Harbor Privacy Principles published by the US Department of Commerce to give a legal framework to the transfer of personal data from the European Union to the United States.

Since this decision has been declared invalid, the company may no longer transfer personal data to the United States on the basis of Safe Harbor.

These facts constitute a violation of Article 68 of French Act no.78-17 of January 6, 1978, as amended, which states that "*The data controller may not transfer personal data to a State that is not a Member of the European Union if said State does not provide a sufficient level of the protection of individuals' privacy, liberties and fundamental rights with regard to the actual or possible processing of their personal data.*"

Therefore, FACEBOOK Inc., located at 1601 Willow Road, Menlo Park, CA 94025 (United States), and FACEBOOK Ireland Limited, located at 4 Grand Canal Square, Grand Canal Harbour, Dublin (Ireland), are hereby issued formal notice, to comply with the following within three (3) months from the date of notification of the decision herein and subject to the measures that they may already have adopted:

- **cease compiling the data of account holders for advertising purposes without a legal basis;**
- **cease processing data that is irrelevant, excessive or inadequate with respect to the purposes pursued,** in particular cease to ask account holders to prove their identity by providing medical records;
- **obtain the explicit consent of account holders,** based on specific information, **for the collection and processing of their "sensitive" data** – for the case at hand, data concerning political and religious views and sexual orientation - **by any means, such as a check box located where information is entered;**
- **inform account holders, in accordance with the provisions of Article 32 of the French Act of January 6, 1978, as amended:**
    - with regard to the processing of personal data, directly on the sign up form and the pages where account holders can complete their profile;

- with regard to the nature of data transferred outside the European Union, the purpose of the transfer, the recipients of said data, and the level of protection offered by third countries;

- **fairly collect and process data of non-account holders with regard to data collected using "datr cookie" and "like button";**
- **inform Internet users and obtain their prior consent for placing information on their terminal device (cookies) and accessing it.** In this regard, the company must, unless it implements a system that gives the same guarantees, provide prior information to Internet users in a clear and thorough manner on the banner on the website:
  - on the purposes of all cookies requiring consent;
  - on the fact that they have the option to change cookie settings by clicking the link in the banner. This banner must redirect to a page that presents adequate solutions for accepting or blocking cookies;
- **cease retaining personal data beyond the length of time required for the purposes for which it was collected and processed,** in particular bydeleting the IP addresses used by account holders to connect to their accounts after 6 months;
- **take all measures necessary to ensure the security of account holder personal data,** in particular by increasing the complexity of account passwords (passwords composed of at least eight characters of 3 different types from the following 4: digits, uppercase letters, lowercase letters, special characters);
- **complete prior formalities applicable to processing, and in particular issue an authorization** request for all data processing with the purpose of preventing fraud and potentially banning users;
- **cease transferring personal data towards the United States on the basis of Safe Harbor;**
- **demonstrate to CNIL that all the aforementioned requests have been complied with, within the allocated time.**

After this deadline, if FACEBOOK Inc. and FACEBOOK Ireland Limited have complied with the formal notice herein, proceedings shall be considered closed, and they shall be sent a letter to that effect.

However, if FACEBOOK Inc. and FACEBOOK Ireland Limited have not complied with the formal notice herein, a reporting judge (*rapporteur)* may be appointed and request that a CNIL restricted committee pronounce one of the sanctions set out in Article 45 of the French Act of January 6, 1978, as amended.

The Chair

Isabelle FALQUE-PIERROTIN