Office of the Data Protection Commissioner.
Canal House, Station Road
Portarlington , Co. Laois
IRELAND

[redacted]
AUSTRIA

Vienna, 18th of August 2011

Complaint against Facebook Ireland Ltd. – 12 "Data Security"

To whom it may concern,

This is a formal complaint against "Facebook Ireland Ltd." under section 10 of the Irish DPA. I am convinced that "Facebook Ireland Ltd." breaches the Irish DPA and the underlying Directive 95/46/EG and I kindly ask you to investigate the following complaint.

I am a user of "facebook.com". The contract is governed by the "terms" used by Facebook (attachment 01). They state in section 18.1. that all users that live outside of the United States of America or Canada, have a contract with Facebook Ireland, while all users within the United States of America and Canada have a contract with Facebook Inc., based in California, United States of America (further called "Facebook USA").

Therefore I do have a contract with "Facebook Ireland Limited, Hanover Reach, 5-7 Hanover Quay, Dublin 2, Ireland" (further on called "Facebook Ireland"). For preforming my contract with them, Facebook Ireland is processing my personal data in different means. Since this controller is established in Ireland, I understand that according to section 3B(a)(i) DPA the Irish Data Protection Act (DPA) applies.

Because facebook.com is similar to a "cloud" service, I want to distinguish between the mere "hosting" of my data and all further processing of my data. For the purpose of hosting my data I see Facebook Ireland as a processor and myself as the controller. For any form of further processing of my data for Facebook Ireland's own purposes (e.g. analytics or advertisement) I see Facebook Ireland as the sole controller (see graphic in attachment 02).
Generally all my hosted personal data is also used for Facebook Ireland's purposes, which is why Facebook Ireland must always be seen as a controller. Whenever Facebook Ireland processes data that was "removed" by the user, it is obvious that the user is not in control of the data; therefore Facebook Ireland is the sole controller at this time. Facebook USA must be seen as the sub-processor or the processor in each case.

Unfortunately Facebook Ireland does not have a certain structure in its processing that would make it easy to distinguish certain forms of processing. In order to make the handling of my complaints easier for you, I decided to split them into individual cases. I want to inform you that some cases are overlapping to a certain extent.

**Case 12 – Data Security**

Facebook Ireland holds excessive amounts of highly personal information. This includes personal messages, relationships, comments, a list of interests, religious and political beliefs, location information or visited events (including events that e.g. indicate political, religious or sexual preferences).
Depending on the political system a user is living in and on the specific content of the information, this bears tremendous security risks for the user. The mere fact that a user is or was "friends" with a person, has interacted with a person, or has been invited to an event (such as demonstrations) might be very risky for the individual user.
But even the mere masses of "normal" information that is saved on Facebook Ireland's servers makes attacks by hackers, identity thieves or secret services very likely. It seems to be only a matter of time until someone finds a way to access Facebook Ireland's data, just like it has happened to many other companies before.

**A) Encryption**
Despite these facts, according to its privacy policy, Facebook Ireland only seems to be encrypting passwords and credit card numbers (see attachment 03). This is questionable, since all other private information would not even be encrypted when a security breach would occur.

**B) Statements**
In addition to that, Facebook Ireland gives the following statements in its terms and privacy policy:

1. *"We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available."*

2. *"We do our best to keep Facebook safe, but we cannot guarantee it."*

3. *"WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES (…) WE DO NOT GUARANTEE THAT FACEBOOK WILL BE SAFE OR SECURE."*

4. *"FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES."*

5. *"WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS."*

These statements make it very questionable if Facebook Ireland is seriously protecting personal information. In fact, they are not even claiming that they are protecting it; they are straight out saying that they do not guarantee any security.

**C) Applications and "Skimming"**
Facebook Ireland is allowing and promoting third party "applications". These applications allow third parties, which might not even fall under the European privacy system, or any equivalent scheme (such as the Safe Harbor Agreement). There are some general provisions that developers of applications have to follow, but even the most basic provisions (such as providing some kind of privacy policy) are not consequently enforced by Facebook Ireland. Since every user can grant an application access to all information his/her friends are sharing

with him/her, these applications bare a tremendous risk for data security. I could not think of another data controller that gives third parties such a broad and uncontrolled access to personal data.

A lot of information is automatically shared with “everyone” on the internet, some information has the be shared with “everyone”. This bares a high risk of “skimming”. An example would be the project of two artists that imported the faces and names of millions of Facebook Ireland’s users for “lovelyfaces.com”.

The facts listed above and the statements of Facebook Ireland make it more than questionable if Facebook Ireland is really securing the user’s data in a way that is sufficient under section 2(1)(d) and section 2C DPA and Article 16 and 17 of Directive 95/46/EG. This seems to be especially questionable if you look at the mere amount of information, the possible sensitivity of it and the rather easy access to the stored information.

I therefore kindly ask you to investigate the security practice by Facebook Ireland further and take further steps (if necessary) to ensure a sufficient level of data security.

I can be reached at [redacted] or [redacted] if you have any further questions.

Sincerely,

[redacted]