REVIEW OF EUROPE-V-FACEBOOK COMPLAINTS IN LIGHT OF THE AUDIT BY THE IRISH DPC

Nature of Complaint	Facebook comments
Complaint 1 – Pokes A poke is a type of short message sent from one Facebook user to another. Complainant stated that while Facebook allows for the removal of old pokes, they are not, in fact, being deleted.	Facebook understands the complaint to related to concerns that there was insufficient transparency for users about what happens with historic poke data and a lack of user control over historic poke data in their accounts. Facebook believes that the plans set out below in response to the findings of the audit by the Irish DPC answer both of these concerns and will therefore provide for the complaint to be resolved. *Relevant sections from audit report –* *Finding* The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved. *Commitment* FB-I will comply with this recommendation in an updated Data Use Policy (by end of Q1 2012). *Finding* Users should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to in so far as is reasonably possible delete on a per item basis. *Commitment* FB-I will phase in such transparency and control to users on a regular basis (demonstrable progress to be shown by July 2012).
Complaint 2 – Shadow Profiles Complainant contended that Facebook is gathering information in relation to non Facebook	Facebook has made it clear that it does not create profiles of non-users. Facebook gave the Irish DPC privileged access to its systems and they were able to verify that we do not build

users. This information primarily consists of email addresses, but may also include names, telephone numbers and addresses. Facebook typically collects this information when a user synchronises their phone or imports their email contact list to their Facebook account. Complainant contended that Facebook is using this data to create profiles of non-users.	"shadow profiles" of the kind described. Facebook therefore regards this complaint as resolved on the basis of these additional facts. *Relevant sections from audit report –* *Finding* We are satisfied that, aside from storage of synchronised data for its users, FB-I makes no additional use of telephone numbers or other contact details uploaded as part of the synchronisation feature unless the user chooses to supply email addresses for friend finder, i.e., sending personal email or SMS invitations, purposes.
Complaint 3 – Tagging Friends on Facebook have the facility to 'tag' photos of another user (friend) and display them on their Facebook page and within the 'news feed' section. While the other user may subsequently remove the tag, the issue is that the user is unable to prevent friends tagging photos to their Facebook page in the first place.	Facebook does not believe that there is any incompatibility between photo tagging per se and Irish data protection law. Rather, Facebook regards photo-tagging as a privacy-enhancing feature as it alerts individuals to the existence of photos of themselves that have been posted on the service. Facebook therefore regards this complaint as resolved. Facebook is however also keen to consider best practice and will work with the DPC in response to their request described below to look further into aspects of user control of this feature and will report back in due course. *Relevant sections from audit report –* *Finding* There does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it. *Commitment.* FB-I will examine the broader implications of this recommendation and will engage further on this issue in the July 2012 review
Complaint 4 – Synchronising This is related to Complaint 2. When a Facebook user synchronises their mobile phone or other device with Facebook, the complainant states	Facebook has clarified in the course of the audit that the information that is uploaded through device synchronisation is only used to send invitations at the request of the user. With this clarification Facebook believes that the part of the complaint concerning invitations is

that all personal data on the device are transferred to Facebook. This may result in invitations being issued by Facebook to those individuals whose data have been transferred. The individuals are not aware that their personal data has been disclosed in this way.	resolved. Facebook also confirmed that the synchronised data is always under the control of the user owning the device who can delete it at any time. Facebook does not believe that there is a legal basis for requiring an individual with a mobile device to notify the people in their personal address book about how they synchronise this data across address books in the different services they use both on and off the device. *Relevant sections from audit report –* *Finding* DPC was satisfied that, aside from storage of synchronised data for its users, FB-I makes no additional use of telephone numbers or other contact details uploaded as part of the synchronisation feature unless the user chooses to supply email addresses for friend finder purposes. *Finding* DPC confirmed that passwords provided by users for the upload of contact lists for friend-finding purposes are held securely and destroyed *Finding* DPC recommended that users be made aware that where they choose to synch their contact information from a mobile device, those contact details are transmitted in plain text and are therefore not secure during transmission. This is not an issue within Facebook's control but users should nevertheless be made aware when choosing this option. *Facebook Commitment* It is not more risky to send data in plain text via the synchronization process than doing so by sending email using an internet email provider, which providers do not provide disclosures on security risks. FB-I will have further dialogue in order to work towards reviewing alternatives for reducing risk and addressing them through education or changes in the product. *Finding* DPC established that the action of disabling synchronisation does not appear to delete any of the synchronised data. This requires an additional step via the "remove data" button within the

	app. We recommend that it should be clear to users that disabling synching is not sufficient to remove any previously synched data. *Facebook Commitment* It should be obvious to users that their synchronized data is still there after they disable synching but FB-I will add text to that effect within the app.
Complaint 5 – Deleted Posts Facebook provides a facility whereby a user can delete old posts. The complainant stated that, while the act of deleting a post does remove the post from view, it is not, in fact, deleted.	Facebook has been working on its data deletion routines to ensure that they fully remove all posts that a user has chosen to delete. Facebook believes that it has resolved this complaint with the measures it has already taken in this area and the further improvements that it has committed to and which are set out below. *Relevant sections from audit report –* *Finding* The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved. *Facebook Commitment* FB-I will comply with this recommendation in an updated Data Use Policy (by end of Q1 2012). *Finding* Users should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to, in so far as is reasonably possible, delete on a per item basis. *Facebook Commitment* FB-I will phase in such transparency and control to users on a regular basis (demonstrable progress to be shown by July 2012).
Complaint 6 – Posting on other Peoples Pages When posting a comment on another person's Facebook page, the information posted is subject	Facebook does not believe that there is any incompatibility between comments being treated in the way described and Irish data protection law. It is very clear to users of the service that the audience for content is controlled by the person who owns the wall where it is posted.

to the other person's privacy settings. The issue for the complainant is that the person posting the comment is unaware of the other user's privacy settings and, accordingly, will not know who can see the comment being posted – it could be restricted to friends only, but equally, could be viewed by everyone on the internet, including search engines.	Facebook therefore regards this complaint as resolved. Facebook is however also keen to consider best practice and will work with the DPC in response to their request to look further into how users can be given even more information about the audience for comments and report back. Facebook notes that with Timeline, it has provided users with the ability to see the audience for posts on others' timelines; therefore, before commenting on a post, the user knows the audience. *Relevant sections from audit report –* *Finding* The DPC recommended that FB-I introduce increased functionality to allow a poster to be informed prior to posting how broad an audience will be able to view their post and that they be notified should the settings on that profile be subsequently changed to make a post that was initially restricted available to a broader audience. The DPC recommended the sending of a notification to the poster of any such change with an ability to immediately delete their post if they are unhappy. *Facebook Commitment* FB-I will examine the broader implications of the suggested approaches and having done so will engage further on this issue in the July 2012 review.
Complaint 7 – Messages It is possible for Facebook users to send instant messages to other users who are online. It is also possible to delete these messages if the user so chooses. However, the complainant contended that the act of hitting the delete button provided merely removes the message from view and does not, in fact, delete it.	Facebook will clarify the effect of a user removing instant messages in the revision to the Data Use Policy as described below. With this measure Facebook regards this complaint as resolved. *Relevant sections from audit report –* *Finding* The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved. *Facebook Commitment* FB-I will comply with this recommendation in an updated Data Use Policy (by end of Q1 2012).

	Finding Users should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to, in so far as is reasonably possible, delete on a per item basis. *Facebook Commitment* FB-I will phase in such transparency and control to users on a regular basis (demonstrable progress to be shown by July 2012).
Complaint 8 – Consent and Privacy Policy There are a number of aspects to this complaint set out under the following headings: ***Access***: the complainant stated that Facebook's Privacy Policy is not easily accessible – the link 'privacy' provided at the bottom of the user's Facebook page is merely a link to a privacy guide, containing limited information. There is a link within this document to the actual Privacy Policy. ***Role of FB-I and the User***: the complainant stated that the user is not provided with any clear information on who is data controller (Facebook Irl. or Facebook Inc). ***Extent of Privacy Information***: the complainant was dissatisfied that, in order to get a grasp of Facebook's privacy policies, a user must deal with multiple documents and links, with many specific provisions difficult to locate. ***Contradictions***: the complainant highlighted contradictions he has identified within the Privacy Policy. He stated that the contradictions identified run to 6 pages and has provided some sample issues in the complaint in relation to the deletion of data.	Facebook does not believe that there is any incompatibility between its current approach to its Data Use Policy and consent process and Irish data protection law. Facebook has however agreed with the Irish DPC to make further improvements as set out below to ensure that users have easy access to our Data Use Policy and that it is easy for them to understand. Facebook notes that the Privacy Policy link has been moved to the right hand side of the user's homepage and that it links directly to the Data Use Policy. Relevant sections from audit report – *Finding* FB-I must work towards: - simpler explanations of its privacy policies - easier accessibility and prominence of these policies during registration and subsequently - an enhanced ability for users to make their own informed choices based on the available information *Facebook Commitment* FB-I will work with the DPC's Office to achieve the objectives of simpler explanations of its Data Use Policy, identify a mechanism to provide users with a basis to exercise meaningful choice over how their personal data is used, easier accessibility and prominence of these policies during and subsequent to registration, including making use of test-groups of users and non-users as appropriate.

Vague Provisions: the complainant has highlighted a number of provisions in the Privacy Policy which he considered to be vague and general in nature. ***Unambiguous Consent***: the complainant has highlighted a number of issues with the process of consenting to the Privacy Policy including the use of small text and lack of a check box to be ticked. ***Freely Given Consent***: this complaint is in relation to the monopoly Facebook has on business and personal users and that there should be a high bar in terms of privacy terms and conditions given the limited competition. ***Specific Consent***: the complainant contended that there is no specific consent being provided by users for the use of their personal data. ***Informed Consent***: the complainant considered that the purpose for which personal data is processed is not properly explained. ***Consent obtained by deception or misinterpretation***: this again relates to how Facebook uses personal data and the complainant has highlighted a number of examples where he considered Facebook to be providing false or misleading information.	*Finding* The relative size of the links to the privacy policy and statement of rights and responsibilities on the second page of the sign up process must be aligned with the other information presented on that page. *Facebook Commitment* Agreed. Furthermore, FB-I has agreed to take the additional step of moving the links to the Data Use Policy and other policy documents, as well as the Help Center, to the left side of the user's homepage (by end of February 2012).
Complaint 9 – Face Recognition In relation to Facebook's use of tagged photos, the complainant contended that there has never been a specific consent provided to users availing of this feature, and particularly in relation to users who would have provided consents to Facebook prior to the introduction of the feature.	Facebook does not believe that specific consent was required under Irish data protection law for the introduction of the tag suggest feature. The Irish DPC audit report confirmed Facebook's view on the lawfulness of the feature. Facebook therefore regards this complaint as resolved The Irish DPC requested that additional notification be offered about this feature as a matter of best practice. Facebook agreed to this and has already implemented the mechanism for providing further notification agreed with the DPC.

	Relevant sections from audit report – *<u>Finding</u>* FB-I should have handled the implementation of this feature in a more appropriate manner and we recommended that it take additional steps from a best practice perspective to ensure the consent collected from users for this feature can be relied upon *<u>Facebook Commitment</u>* FB-I will provide an additional form of notification for Tag Suggest. It will appear at the top of the page when a user logs in. If the user interacts with it by selecting either option presented then it will disappear for the user. If the user does not interact with it then it will appear twice more for a total of 3 displays on the next successive log-ins. Before making a selection more detail about how the feature works will appear behind a Learn More link and will also be shown if a user clicks Adjust Your Settings (by first week of January 2012). FB-I will discuss with the DPC's Office any plans to extend tag suggest to allow suggestions beyond confirmed Friends in advance of doing so.
Complaint 10 – Access Requests This complaint relates to an incomplete access request. The complainant stated that his access request resulted in only limited data being provided. He outlined the areas - 19 of them - under which he contended Facebook did not provide information.	Facebook has carried out a thorough review of the types of data it holds and how these might be accessed by the user. This has resulted in an agreed schedule of work with the Irish DPC to deliver a schema that meets the requirements of Irish data protection law. Facebook notes that Timeline and activity log, both new features, provide access to numerous additional categories of user data. *Relevant sections from audit report –* *<u>Finding</u>* If identifiable personal data is held in relation to a user or non-user, it must be provided in response to an access request within 40 days, in the absence of a statutory exemption *<u>Facebook Commitment</u>* FB-I will fully comply with the right of access to personal data, as outlined in the schedule above. It has additionally committed to a key transparency principle that users are entitled to have easy and effective access to their personal information.
Complaint 11 – Removal of Tags A user is provided with the option 'remove tag'	Facebook has explained that it is necessary to retain data about a deleted tag in order to

from a tagged photo on their Facebook page. However, the complainant contended that removing the tag is not deleting the tag data and that Facebook is not transparent in terms of informing users on the retention of this information following the use of the 'remove tag' option.	prevent the photo from being re-tagged against the person's wishes. Facebook will make this fact transparent in a revision to its Data Use Policy. Facebook believes that this complaint will be resolved with the provision of such additional information. *Finding* The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved. *Facebook Commitment* FB-I will comply with this recommendation in an updated Data Use Policy (by end of Q1 2012). *Finding* Users should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to in so far as is reasonably possible delete on a per item basis. *Facebook Commitment* FB-I will phase in such transparency and control to users on a regular basis (demonstrable progress to be shown by July 2012).
Complaint 12 – Data Security The complainant set out a number of security concerns in relation to the security of personal data – no encryption on private data (other than passwords and credit cards), not taking enough responsibility for data security in its privacy statements and a lack of control over data being provided to third party applications.	Facebook believes that the audit report demonstrates that FB-I has in place adequate data security policies and practices under Irish data protection law. Facebook has agreed to the following commitments with the DPC in this area to further improve its practices. Facebook therefore believe that this complaint is resolved. *Relevant sections from audit report –* *Finding* Many policies and procedures that are in operation are not formally documented. This should be remedied. *Facebook Commitment* FB-I will continue to document policies and procedures as required to maintain consistency in security practices.

	Finding DPC was satisfied that FB-I does have in place an appropriate framework to ensure that all access to user data is on a need to know basis. However, the DPC recommended that FB-I expand its monitoring to ensure that there can be no employee abuse through inappropriate password resets of a user's account *Facebook Commitment* FB-I will integrate user password resets by employees into our monitoring tools *Finding* DPC expressed concern that the tools in place for ensuring that staff were authorised to only access user data on a strictly necessary basis were not as role specific as the DPC would have wished. *Facebook Commitment* FB-I is implementing a new access provisioning tool that will allow for more fine-grained control of access to user data. Facebook believes that current arrangements adequately mitigate the risk of large-scale harvesting of Facebook user data via "screen scraping" while allowing the service to be effectively provided to legitimate users.
Complaint 13 – Applications This relates to third party applications which sit on the Facebook Platform. The complainant outlined a number of issues including a lack of informed user consent when accessing a third party application, a lack of oversight by Facebook in terms of privacy compliance among third parties and the non-notification to users by Facebook in a case where a third party has no privacy policy.	Facebook does not believe that there is any incompatibility between its current approach to offering a platform for users to install applications of their own volition and Irish data protection law. These issues were examined during the course of the audit and the DPC found that safeguards were in place. Facebook has agreed to a number of measures to further improve the transparency of data handling by applications. Facebook believes that with this additional information this complaint is resolved. *Relevant sections from audit report –* *Finding* DPC verified that it was not possible for an application to access personal data over and above that to which an individual gives their consent or enabled by the relevant settings. *Finding*

	The complexity for a user to fully understand in a meaningful way what it means to grant permission to an application to access their information must be addressed. Users must be sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications *Facebook Commitment* FB-I has recently changed its granular data permissions dialog box for apps, which was expected to be fully available on all applications in February 2012, to allow for contextual control over the audience that will see the user's activity on Facebook. *Finding* It must be made easier for users to understand that their activation and use of an app will be visible to their friends as a default setting *Facebook Commitment* FB-I has recently changed its granular data permissions dialog box for apps where users can choose the audience ("audience selector") for their app activity directly in the dialog box. *Finding* The privacy policy link to the third party app should be given more prominence within the application permissions screen and users should be advised to read it before they add an app. This should be supplemented with a means for a member to report a concern in this regard via the permissions screen. *Facebook Commitment* There is a "report app" link in every dialog box, which permits users to notify FB-I of any issues regarding the app, including a missing or non-working privacy policy link. In addition, FB-I will further educate users on the importance of reading app privacy policies and is positively disposed to increasing the size of the link in the dialog box and will report back to the DPC's Office. *Finding* As the link to the privacy policy of the app developer is the critical foundation for an informed consent, FB-I should deploy a tool that will check whether privacy policy links are live. *Facebook Commitment* FB-I will implement this recommendation and is urgently examining how to introduce this feature from a technical feasibility perspective (progress to be examined in July 2012 visit).

	Finding DPC verified that when a friend of a user installing an app has chosen to restrict what such apps can access about them that this cannot be over-ridden by the app. However, it should be made easier for users to make informed choices about what apps installed by friends can access personal data about them. The easiest way at present to manage this is to turn off all apps via a user's privacy settings but this also prevents the user from using apps themselves. *Facebook Commitment* FB-I will positively examine alternative placements for the app privacy controls so that users have more control over these settings *Finding* DPC identified that the authorisation token granted to an application could be transferred between applications to potentially allow a second application to access information which the user had not granted by way of the token granted to the first application. While this is a limited risk the DPC recommended that FB-I bring forward a solution that addresses the concerns outlined. In the meantime, at a minimum the DPC expected FB-I to advise application developers of their own responsibility to take appropriate steps to ensure the security of the authorisation tokens provided by it. *Facebook Commitment* FB-I will provide more messaging to developers highlighting its policy regarding sharing of authorization tokens. In addition, FB-I will commit to investigate technical solutions to reduce risk of abuse (notifications to developers by end of January 2012, technical solution to be presented by end of Q1). *Finding* The DPC does not consider that reliance on developer adherence to best practice or stated policy in certain cases is sufficient to ensure security of user data. The DPC does note however Facebook's proactive monitoring and action against apps which breach platform policies. However, this is not considered sufficient by the DPC's Office to assure users of the security of their data once they have third party apps enabled. The DPC expects FB-I to take additional steps to prevent applications from accessing user information other than where the user has granted an appropriate permission. *Facebook Commitment* FB-I has proactive auditing and automated tools designed not just to detect abuse by

	developers, but to prevent it in the first place and the findings of the audit will be used to further refine the tools.
Complaint 14 - Removed Friends Facebook provides a facility to add friends and to 'unfriend' friends. The issue here is that when a user clicks on the 'unfriend' option, the friend information is not deleted, but is retained in the background – the complainant saw no justification for the retention and considered that Facebook is not transparent in terms of informing users on the retention of the information.	Facebook has explained that it is necessary to retain data about a removed friend in order to prevent the former friend from sending repeated friend requests against the person's wishes. Facebook will make this fact transparent in a revision to its Data Use Policy. Facebook believes that this complaint will be resolved with the provision of such additional information. *Relevant sections from audit report –* *Finding* The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved. *Facebook Commitment* FB-I will comply with this recommendation in an updated Data use Policy (by end of Q1 2012). *Finding* User's should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to in so far as is reasonably possible delete on a per item basis. *Facebook Commitment* FB-I will phase in such transparency and control to users on a regular basis (demonstrable progress to be shown by July 2012).
Complaint 15 – Excessive Processing This covers a number of earlier complaints in terms of the non-deletion of information (pokes, tags, etc.) which a user may have removed from their page. The complainant considered the amount of data Facebook holds and processes to	Facebook does not accept that its data processing activities are incompatible with Irish data protection law. Facebook is committed to improving transparency about processing in its Data Use Policy. Facebook is also committed to working with the Irish DPC to ensure that its data retention and deletion policies are effective and consistent with the expectations of the DPC and has made a number of commitments as set out below. Facebook believes that with the

be excessive and a security risk.	information provided in the audit report and these additional actions that this complaint will be resolved. *Relevant sections from audit report –* *Finding* The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved. *Facebook Commitment* FB-I will comply with this recommendation in an updated Data Use Policy (by end of Q1 2012). *Finding* Users should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to, in so far as is reasonably possible, delete on a per item basis (demonstrable progress to be shown by July 2012). *Facebook Commitment* FB-I will phase in such transparency and control to users on a regular basis. *Finding* Data held in relation to inactive or deactivated accounts must be subject to a retention policy. *Facebook Commitment* FB-I will work with this Office to identify an acceptable retention period. *Finding* Personal data collected must be deleted when the purpose for which it was collected has ceased. *Facebook Commitment* FB-I will comply with requirements in relation to retention where the company no longer has a need for the data in relation to the purposes for which it was provided or received. Specifically: 1. for people who are not Facebook users or who are Facebook users in a logged out state, FB-I will take two steps with respect to the data that it receives and records through social plugins within 10 days after such a person visits a website that contains

	a social plugin. First, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com. 2. for all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin. 3. anonymise all search data on the site within six months 4. anonymise all ad click data after 2 years 5. significantly shorten the retention period for log-in information to a period which was agreed with the DPC's Office.
Complaint 16 – Opt Out The complainant argued that there is no specific consent when signing up to Facebook (see check box issue in Complaint 8) and that personal data is being collected prior to a new user being able to set their privacy settings. The complainant also contended that the security settings themselves are too liberal in nature and that the settings pages and links provided discourage the new user from applying certain security settings.	Facebook does not believe that there is any incompatibility between its current approach to its Data Use Policy and Irish data protection law. Facebook has however agreed with the Irish DPC to take make further improvements as set out below to ensure that users have easy access to its Data Use Policy and that it is easy for them to understand. *Relevant sections from audit report –* *Finding* FB-I must work towards: - simpler explanations of its privacy policies - easier accessibility and prominence of these policies during registration and subsequently - an enhanced ability for users to make their own informed choices based on the available information *Facebook Commitment* FB-I will work with the DPC's Office to achieve the objectives of simpler explanations of its Data Use Policy, identify a mechanism to provide users with a basis to exercise meaningful choice over how their personal data is used, easier accessibility and prominence of these

	policies during and subsequent to registration, including making use of test-groups of users and non-users as appropriate. *Finding* The relative size of the links to the privacy policy and statement of rights and responsibilities on the second page of the sign up process must be aligned with the other information presented on that page. *Facebook Commitment* Agreed. Furthermore, FB-I has agreed to take the additional step of moving the links to the Data Use Policy and other policy documents, as well as the Help Center, to the left side of the user's homepage (by end of February 2012).
Complaint 17 – Like Button The complainant stated that when a user visits a website which contains a 'social plug in' – the Like button – the following information is being recorded: date, time, URL, IP address, browser and operating system information. The complainant considered that the information is being collected unfairly and is excessive.	Facebook does not accept that its data processing activities are incompatible with Irish data protection law. Facebook is committed to improving transparency about processing in its Data Use Policy. Facebook is also committed to working with the Irish DPC to ensure that its data retention and deletion policies are effective and consistent with the expectations of the DPC and has made a number of commitments as set out below. Facebook believes that with the information provided in the audit report and these additional actions that this complaint will be resolved. *Relevant sections from audit report –* *Finding* DPC was satisfied that no use is made of data collected via the loading of Facebook social plug-ins on websites for profiling purposes of either users or non-users. *Finding* Personal data collected must be deleted when the purpose for which it was collected has ceased *Facebook Commitment* FB-I will comply with requirements in relation to retention where the company no longer has a need for the data in relation to the purposes for which it was provided or received. Specifically:

	1. for people who are not Facebook users or who are Facebook users in a logged out state, FB-I will take two steps with respect to the data that it receives and records through social plugins within 10 days after such a person visits a website that contains a social plugin. First, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com. 2. for all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it receives and records through social plugin impressions within 90 days after a person visits a website that includes a social plugin. 3. anonymise all search data on the site within six months 4. anonymise all ad click data after 2 years 5. significantly shorten the retention period for log-in information to a period which was agreed with the DPC's Office *Finding* It is not appropriate for Facebook to hold data collected from social plug-ins other than for a very short period and for very limited purposes. *Facebook Commitment* Impression data received from social plugins will be anonymised within 10 days for logged-out and non-users and deleted within 90 days, and for logged-in users, the data will be aggregated and/or anonymised in 90 days.
Complaint 18 – Obligations as Processor The complainant considered that FB-I is a data	Facebook does not believe that the model described in this complaint for the controller-

processor while the Facebook user is the data controller. He contended that Facebook's operation as a processor is at variance with both Irish Data Protection legislation and Directive 95/46/EG.	processor relationship is supported by the facts. Facebook therefore believes the complaint is resolved.
Complaint 19 – Pictures Privacy Settings Facebook allows a user to upload photographs to their Facebook page and apply security settings. The complainant stated that Facebook has outsourced the delivery of the picture content to a company (Akamai Technologies) and, by using the source code from the pictures page of Facebook.com and identifying certain URLs, that it is possible to view some photos that should be hidden from view.	Facebook believes that its use of caching services is consistent with industry best practice and with Irish data protection law. The audit confirmed that any privacy threat as outlined in the complaint is not realistic. Facebook therefore believes this complaint has been resolved. *Relevant sections from audit report –* *Finding* The DPC was satisfied that there is no realistic security threat to a user photo from their upload to Akamai. DPC was also satisfied that there is no realistic threat to a deleted image.
Complaint 20 – Deleted Pictures This complaint relates to the previous complaint (19). Facebook users are given the option to delete pictures they have uploaded to Facebook. Again, by using the source code from the pictures page of Facebook.com and identifying certain URLs, the complainant stated that it was possible to view a photograph for up to 48 hours after he had deleted it from Facebook.	Facebook believes that its use of caching services is consistent with industry best practice and with Irish data protection law. The audit confirmed that any privacy threat as outlined in the complaint is not realistic. Facebook therefore believes this complaint has been resolved. *Relevant sections from audit report –* *Finding* The DPC was satisfied that there is no realistic security threat to a user photo from their upload to Akamai. DPC was also satisfied that there is no realistic threat to a deleted image.
Complaint 21 – Groups Facebook allows users to add friends to groups which are found on the user's Facebook page and within 'news feeds'. The issue raised in the complaint is that a user can be added to other users groups without their consent.	Facebook does not believe that there is any incompatibility between the way in which Groups operate on the service and Irish data protection law. Facebook has however agreed as a matter of best practice to make changes to the process of being added to a Group such that users will not be represented as members of a Group until they visit the Group page and are given the opportunity to immediately leave the Group. Facebook believes that with the action set out below this complaint will be resolved.

	Relevant sections from audit report – *<u>Finding</u>* Users must be provided with a means to exercise more control over their addition to Groups *<u>Facebook Commitment</u>* FB-I has agreed that it will no longer be possible for a user to be recorded as being a member of a Group without that user first visiting the Group page and being given an opportunity to immediately leave the Group. . (By end of Q1 2012).
Complaint 22 – New Policy This relates to recent changes made to Facebook's Privacy Policy. The complainant contended that it is difficult to understand the changes in conjunction with the previous policy and that users have not had any opportunity to consent to the changes made.	Facebook does not believe that there is any incompatibility between its current approach to its Data Use Policy and Irish data protection law. Facebook has however agreed with the Irish DPC to take make further improvements as set out below to ensure that users have easy access to our Data Use Policy and that it is easy for them to understand. *Relevant sections from audit report –* *<u>Finding</u>* FB-I must work towards: - simpler explanations of its privacy policies - easier accessibility and prominence of these policies during registration and subsequently - an enhanced ability for users to make their own informed choices based on the available information *<u>Facebook Commitment</u>* FB-I will work with the DPC's Office to achieve the objectives of simpler explanations of its Data Use Policy, identify a mechanism to provide users with a basis to exercise meaningful choice over how their personal data is used, easier accessibility and prominence of these policies during and subsequent to registration, including making use of test-groups of users and non-users as appropriate. *<u>Finding</u>* The relative size of the links to the privacy policy and statement of rights and responsibilities on the second page of the sign up process must be aligned with the other information

	presented on that page. *Facebook Commitment* Agreed. Furthermore, FB-I has agreed to take the additional step of moving the links to the Data Use Policy and other policy documents, as well as the Help Center, to the left side of the user's homepage (by end of February 2012).