Comments from Facebook on the European Commission's proposal for a Regulation "On the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"

This paper sets out the views of Facebook on the European Commission's proposal for a Regulation "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (hereafter referred to as the 'Regulation').

Facebook's mission is to give people the power to share and make the world more open and connected. With over 800 million users worldwide, the impact on people's lives ranging from active participation in political dialogue to personal stories of families being reunited is unprecedented.

Facebook is also a driver of economic growth and job creation: A recent study from Deloitte found that Facebook added more than €15 billion in value in the European Union in 2011, supporting more than 230,000 jobs. In the U.S., a similar study found that applications built on Facebook's platform have contributed at least 182,744 new jobs and over $12.9 billion wages. Facebook therefore welcomes the fact that one of the objectives of the European Commission in proposing the new legislative framework on Data Protection is to foster growth and jobs.

The revision of the Data Protection Directive has the potential to facilitate innovation, and provide consumers with greater transparency and control. Facebook believes that it is possible to have sound privacy regulation and a thriving digital sector. The new legislative framework should focus on encouraging best practices by companies like Facebook rather than on setting out detailed technical rules that will not stand the test of time and may be frustrating and costly for both service providers and users.

Privacy is at the core of everything that we do on Facebook and there are three main principles guiding our privacy programme: transparency, control and accountability. We are **transparent** about how the data users provide is handled by Facebook. This is explained in simple and clear language in our Data Use Policy document (available at www.facebook.com/help). We empower users with **control** over their privacy settings every time they share content. With our 'inline controls' people can choose the audience with which they are sharing content every time they post. When a user chooses to install a new application on Facebook, they are informed via a pop-up window about what data that application needs to access and the user must make an active choice as to whether to accept this data use before installing the application. We hold ourselves **accountable** first and foremost to our users and of course to regulators. All users outside of North America have a contract with Facebook Ireland, which is regulated by the Irish Data Protection Authority (DPA) - the Office of the Irish Data Protection Commissioner (DPC).

This paper addresses ten key aspects of the Regulation indicating which elements Facebook encourages policy makers to consider revising. We suggest that four issues should be prioritised in this respect:

1. ***Jurisdiction/"One-Stop-Shop."*** Facebook welcomes the core principle of a single Data Protection Authority (DPA) having jurisdiction over companies that operate across multiple European countries, but we have concerns about related provisions that could undermine the intent of the principle and create legal uncertainty for businesses.

2. ***Consent.*** Individuals should be able to exercise control over what personal data companies collect from them and how they use it, but the proposed requirement for consent will impair companies' ability to innovate and negatively impact on the individual's experience.

3. ***The Right to Be Forgotten.*** The right to be forgotten, as drafted, raises major concerns with regard to freedom of expression on the Internet. There is also a risk that it could result in technologically impossible obligations. The goal should be to find an appropriate balance between an individual's right to control his or her data, another's right to free expression (to comment about other people), and the practical reality that once information is shared (online or offline) further sharing is difficult to control.

4. ***Privacy by Design/Privacy by Default.*** We believe that industry should be guided by the 'Privacy by Design' principle when building products and services. However, pursuing 'Privacy by Default' does not sufficiently take into account the specific nature of social networking services where people sign up in order to share and connect with others. The Regulation should be revised to take into account the context in which data is collected and processed.

We stand ready to discuss points of detail about how the legislation might be improved with policy makers, Internet user groups and other organisations in the Internet eco-system.

Below is a detailed analysis of the main aspects that Facebook considers would merit improvement during the legislative process:

1. Data Protection Authority (DPA) competence

The core principle of a single DPA having competence across the EU for multinational companies is welcome, though we have concerns about related provisions which could undermine this.

The proposed Regulation provides that the Data Protection Authority (DPA) of the country hosts the European Headquarters of a business it has jurisdiction on behalf of the rest of the EU.

Facebook welcomes this provision and the European Commission's initiative to bring about more harmonization to EU Data Protection legislation and especially DPA jurisdiction by creating a 'one-stop-shop' – ie a single regulatory authority for the whole EU market. Since 2010, Facebook Ireland Ltd has provided Facebook users in Europe with their service, and has been subject to oversight by the Office of the Irish Data Protection Commissioner (DPC), the Irish DPA, for compliance with Irish data protection law.

Facebook is a leader among global Internet service providers in its transparency and willingness to engage with European DPAs and will continue to take this constructive approach to meeting its obligations to its users. Being established in Ireland, Facebook Ireland is regulated by the Irish DPA. Facebook has recently been the subject of a thorough and detailed audit by the Irish DPA, published at our volition on 21 December 2011, on its practices and policies. Substantial resources were dedicated to ensure that the DPA had all the information it needed to conduct a comprehensive audit. The audit involved three months of rigorous examination, and the final DPA report demonstrated Facebook's commitment not only to complying with Irish data protection law but also to adhering to European data protection principles. Facebook believes that practices such as the Irish audit are extremely important in demonstrating compliance with the law and would like to obtain legal certainty that a true 'one-stop-shop' will be applied in Europe.

Article 51 provides that when a data controller and/or data processor is established in several Member States of the European union the responsible DPA will be the one of the main establishment. However, it remains unclear whether the 'one-stop-shop' principle applies in the case where a controller is based outside of the EU.

In the case of Facebook, Facebook Inc. (based in the US) is a data processor for Facebook Ireland. As a data processor not established in the EU, Facebook Inc. is not subject to the Regulation but if Facebook Inc. were also to be regarded as a data controller for the purposes of the Regulation, it would not be able to benefit from the "one-stop-shop" principle. The simplest way of providing the greatest degree of certainty for both international companies and individuals in this respect would be to

amend the rules dealing with the applicability of the law (Article 3), so that where the same processing of personal data takes place in the context of the activities of an establishment of a controller in EU and the activities of a controller within the same corporate group not established in the EU, the EU-based controller would be responsible for EU data protection compliance in respect of the data processing activities taking place within that corporate group. As a consequence, the supervisory authority of the main establishment of the controller in the EU would be competent for the supervision of those data processing activities. Facebook believes that this would enhance the objectives that the European Commission had in mind in ensuring that the 'one-stop-shop' is robust.

Facebook is also concerned that there are a series of articles that undermine the power of the leading DPA, which could lead to inconsistencies and case-by-case decisions in the application of the Regulation and create legal uncertainty for businesses. In particular:

- Mutual assistance - Under Article 55(8), an EU DPA can take a provisional measure, if the lead DPA does not answer their request within one month. The DPA of the main establishment might have legitimate reasons for delaying the adoption of a provisional measure and this should not undermine its competence.

- Joint operations of supervisory authorities (Article 56) - The right for each DPA to participate to joint operations equally raises significant risks with regards to the 'one-stop-shop' principle. As we understand it the proposal is that any EU DPA would have the right to be involved in a joint investigation with the lead DPA. The lead DPA could even confer their investigative and executive power to another DPA. This creates significant legal uncertainty for businesses, which have been dedicating resources to cooperating and dealing with their lead DPA.

- Consistency mechanism (Articles 57 – 63)- These provisions are aimed at ensuring unity of application of the Regulation in relation to processing operations, which may concern data subjects in several Member States. Facebook supports the objective, however some of these provisions raise a risk for the lead DPA having its power undermined by the European Data Protection Board (EDPB), the European Commission and other DPAs. This is another potential area of legal uncertainty for businesses and risks creating long delays in key decisions, which could have a significant impact on innovation cycles.

2. Consent

Users should be able to exercise control over what personal data companies collect from them and how they use it but the requirement for consent should not lead to an overly disrupted or disjointed Internet experience.

The Regulation provides enhanced requirements when controllers rely on data subject consent to legitimize data processing.

It is important to keep in mind that services like Facebook are designed for people to be able to connect and share information. The audit conducted by the Irish DPA at the end of 2011 determined that in the case of a social network, a user provides consent upon registering with the service. Furthermore, Facebook provides extensive information on the site about how information is used and people understand how the service works. In addition, users need to provide their specific and express consent to developers at the time when they download a new application.

The highly prescriptive nature of the requirements for consent contained in Articles 4(8) 7(2) and recital 25 could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk of inundating users with tick boxes and warnings. As well as affecting the user experience, this inevitably will lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it.

Facebook urges policy makers to consider fully the implications of such overly prescriptive provisions that would have an adverse effect on user-experience and could risk undermining the objectives sought.

3. Right to be forgotten

The right to be forgotten needs very careful consideration. As drafted, it raises major concerns with regard to the right of others to remember and of freedom of expression on the Internet. There is also a risk that it could result in measures which are technically impossible to apply in practice and therefore make for bad law. A right balance should be found between data subject's right to get their data deleted, the fundamental rights of other individuals and the reality of the online environment.

The proposal prescribes a right for people to have their data deleted and also requires data controllers to take all reasonable steps to obtain erasure of content copied to a third party website or application. It is important to differentiate between three challenges presented by the 'right to be forgotten':

- The *first* is in relation to people who have posted personal information about themselves online and later wish to delete that information. Facebook believes that in principle this is a right people should have and their decisions should be complied with and respected. Therefore, this is something that Facebook already offers – users can delete individual items of content they have posted on their Timeline including their whole account at any time. In this respect, FB-I is

working with the Irish DPA to provide greater transparency and control to users over the deletion of other information. That said, this may need to be balanced against the rights of others to remember, which, in the context of Facebook, means that some users may wish to retain on their account information posted by others in the past.

- The *second* is in relation to the practical difficulty to identify the necessary information to ensure compliance with the right to be forgotten. This challenge arises in two specific situations:

    - The first situation concerns the deletion of personal data of an individual made available online by another individual. In practice, the operator of a website or hosting platform like Facebook is unlikely to know in very many cases which information available on the platform constitutes the personal data that should be deleted. It is virtually impossible to control what information millions of users may make available about other individuals – many of whom will not be users themselves – and to determine where all of the information is and whether that information is the personal data of the person making the request. Therefore a broad obligation to delete any information made available by users upon request of other individuals would be likely to present major implementation challenges to the extent that it would be practically unworkable.

    - The second situation concerns the specific provision under Article 17(2), which requires informing third parties of the request for deletion of links to or copies of an individual's personal data. This would involve identifying any such links or copies of the information elsewhere on the Internet and communicating with those responsible for placing the links or copying the information to request such links or information to be deleted. Again, we do not see any practicable means for services like Facebook to control which links to or copies of someone's personal data exist in other places on the Internet, let alone communicate with the third parties responsible for their dissemination.

  In order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the Internet. Facebook is strongly concerned that it could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

- The *third* is in relation to any personal data made publicly available and the fact that there may be strong grounds to justify under certain circumstances the right of others to know certain facts concerning individuals, as this is closely linked to the right to freedom of expression and other democratic values. It is clear that there is a potential conflict between the right for people to express themselves and the privacy rights of others. Facebook urges policy makers to consider fully the implications on the open Internet and personal expression as they determine the right balance. The scope of freedom of expression contained in Article 80 and further clarified in Recital 121 is defined quite narrowly and should be extended to cover for example mere expressions of opinion, user generated content and more generally recognise the nature of new forms of communication such as blogging and social networking.

Finally, the debate on the "right to be forgotten" affects a number of Internet services, which rely on user-generated content. This issue is not unique to Facebook or social networking. Policy makers should take into account the "right of others to remember" and reach a balanced conclusion which respects freedom of expression.

4. Privacy by default/privacy by design

'Privacy by design' is a welcome principle but the accompanying 'privacy by default' principle takes insufficient account of the sharing ethos underpinning social network services. The Regulation should have respect for the context in which data is collected and processed.

Facebook welcomes the introduction of the 'privacy by design' principle in Article 23. Privacy is at the core of everything that Facebook does and as part of its work with the Irish DPA, privacy by design, is a key component of its privacy programme.

Facebook believes that people should have control over each piece of content they post. That is why Facebook empowers people with robust tools and educates them with tool tips and confirmation dialogs the first time they share, which helps to ensure that they are sharing with the people they want and that they know how to adjust their settings for the future.

Facebook regrets however that this provision does not take into account the specific nature of social networking where the very reason that most people join is to share and connect with others. Specifically, Article 23 also introduces the notion of 'privacy by default' and requires that, by default, only personal data that are necessary for a specific purpose are to be processed. It further requires that by default 'personal data are not made accessible to an indefinite number of individuals'.

At Facebook, the recommended initial account settings are chosen to allow people to easily find and connect with their friends while protecting more sensitive information. More importantly, with the inline controls introduced in August 2011, people are able to choose their privacy settings each and every time they post content by deciding the audience to whom it is viewable.

Facebook also believes that settings should be age-appropriate. This is why special limitations are in place for users under the age of 18. These automatically limit the under 18's sharing to a much smaller subset of people, which substantially reduces their visibility. Under 18s also cannot have public search listings, so their profiles do not show up in public search engines until they have turned 18.

Facebook therefore suggests that this provision is revisited to take into account services that are expressly designed for the sharing of personal data, such as social networking sites. The Regulation should have respect for the context in which data is collected and processed.

5. Controller/Processor

Proposals regarding the definition of the data controller need to be narrowed down to ensure that companies can operate efficiently with legal certainty.

For the purposes of this Regulation, the data controller for EU Facebook users is considered to be Facebook Ireland Ltd and the data processor is Facebook Inc in California. Facebook would like to maintain the clarity of this structure. Facebook has for a long time fully accepted its responsibility to its users in Europe and since 2010, these users have been provided with their service by Facebook Ireland. This structure is compliant with Irish data protection law and is subject to oversight by the Irish DPA.

Facebook is concerned, however, that the concept of data processor in the Regulation is not clearly defined and, as a result, there may be situations where a data processor may unjustifiably be regarded as a data controller. For example, under Article 26(4), if a processor is considered to be taking independent decisions then that processor will be deemed as a controller. Facebook believes that the interaction between the two concepts might raise practical difficulties when a data controller and a data processor are part of the same company group and both parts of the group collaborate on a daily basis. The policies and protocols will be defined by the data controller, but often implemented independently by the data processor. To avoid any legal uncertainty, Facebook suggests therefore that the definition of data processor is modified to allow certain elements of co-decision-making.

Article 22 introduces new accountability provisions on controllers. These include requirements to demonstrate compliance with the Regulation through the adoption of internal policies, assignment of internal responsibilities and verification of compliance. Facebook agrees with these provisions, however there may be some difficulty in situations where the level of prescription in the Regulation is such that they may not reflect practices that are otherwise appropriate to safeguard personal data. Facebook therefore suggests that this Article requires further consideration by policy makers.

6. Security / Data Breach notification

Consumers should have a right to secure and responsible handling of personal data though there is a risk that the overly prescriptive nature of the Regulation could create a level of bureaucracy that distracts organizations and regulators from achieving the principal objective of securing personal data.

Facebook takes the security of its users very seriously. The Irish DPA commended Facebook on its ongoing focus on the protection and security of user data. It acknowledged that Facebook makes innovative use of technology to identify unusual or suspicious activity on an account. Facebook believes that policy makers should recognize innovative approaches to security. For example Facebook promptly warns users if their account has been compromised. It allows access to the last log-in attempts and provides users with one-time passwords when they log in from unsecured locations. We work closely with analysts, engineers, fraud experts and security investigators to prevent abuse, defeat criminals and help maintain Facebook as a trusted environment.

Facebook is concerned about the overly prescriptive nature of the proposed security provisions and questions whether they add anything to actually enhancing security. Under Article 31 data breaches must be notified to the relevant DPA where feasible within 24 hours. The DPA notification requirement is an absolute requirement, which means that, in theory, even the most minor breaches must be reported to the DPA. Facebook is concerned that this will not allow for effective prioritization of the most serious breaches. The obligations also contain prescriptive requirements for the provision of information to the DPAs, which creates an additional layer of bureaucracy. Furthermore, DPAs may not have appropriate resources to promptly deal with these notifications and this would undermine their effectiveness and the confidence in their role in ensuring that data controllers properly handle important personal data breaches.

Similarly, under Article 32 data breaches need to be notified to data subjects where the breach is likely to adversely affect the personal data or privacy of the data subject. In this instance, the notification must be made without undue delay. This provision raises the same concerns as in Article 31 namely that, the 24 hour deadline is too short, the information to provide to the data subject is extensive and that data breach is not clearly defined.

Furthermore, given the broad definition of data subjects in the Regulation there is a risk that Facebook would be obliged to inform all users who have accessed a page, group or profile that has been compromised. In order to avoid such a costly and cumbersome process, Facebook suggests that the scope of this article is narrowed down.

7. Children

Facebook broadly supports the specific proposals around children and data protection and suggests that a harmonized definition of a *child for the purpose of data processing* is set at under 13.

Facebook believes that Internet services should be designed in an age-appropriate way. Our policy is that you must be 13 to have a Facebook account and there are different privacy settings in place for users aged between 13-17 as described above.

The Regulation defines a "child" as being anyone under 18. Facebook questions whether a general definition is appropriate in the context of this Regulation and whether this is the appropriate age in relation to data processing of a child in all contexts. If the definition is to remain in the Regulation Facebook would recommend a harmonized definition of a child *for the purposes of data processing*, set at the age of under 13, in line with current practices.

Facebook welcomes the specific provision in Article 8 that for online services parental consent is only required for children under 13. Under the same provision "verifiable parental consent" is required "taking into consideration available technology". Although helpful, it is still unclear in what form verifiable consent should take and this is left to be defined by the European Commission at a later date. Facebook believes that many innovative solutions can be found for challenges on the Internet, including the provision of parental consent, and would therefore wish to see these provisions implemented in such a way that they encourage rather than limit this innovation.

Facebook supports initiatives aimed at providing children with specific educational material using simple language, explaining the privacy policy and empowering them to give informed consent about the processing of their data.

8. International data transfers

Facebook welcomes the progress has been made on the international data transfer front. However the Regulation creates several requirements that will be of concern for international organizations.

The Regulation only allows data transfers outside of the EEA if the conditions set out in Articles 40-41 are complied with.

As with the current Directive, transfers to non-EEA territories with an adequacy finding are permitted. Under A41 (3) and (5) the European Commission can decide that a country, but also, an organization (for example, a private company) does not meet the adequate level of protection. The current practice is that for Facebook the Irish DPA is responsible for deciding the adequacy of a private organization to execute international transfers and this should remain the case.

To ensure the compliance of its international data transfers, Facebook employs different mechanisms including: users' consent; strong data transfer clauses in its data processing agreement; and also relies on the EU-US Safe Harbor Agreement. The Safe Harbor agreement has helped many start-up companies grow and offer their services to more people in the confidence that their legal obligations are met. Facebook has for a long time fully accepted its responsibility to its users in Europe and participated in the EU-US Safe Harbor Agreement for data processing for several years. This was a good way to meet its obligations to protect the privacy rights of users in the EU before it had its operations well established in Europe. A recognition of the Safe Harbor agreement in the Regulation would be welcomed.

Facebook is also concerned about the extra layer of bureaucracy, which is created by the requirement under Article 42(4). This refers to the situation in which the contractual clauses included in the data processing agreement are not standard and the controller is required to get the prior authorization from the lead authority (Article 34), or from the European Data Protection Board (Articles 57, 58).

Finally, Article 44 specifies the derogations from the general prohibition on international data transfers. The data transfer will be authorized if (1) it is based on a legitimate interest of the controller or processor and (2) the transfer cannot be qualified as frequent or massive, and (3) the controller or processor has assessed all the circumstances and adduced appropriate safeguards with respect to the protection of personal data. Whilst this is a positive development, the reference to "not being frequent or massive" reduces the potential beneficial effect of allowing organizations to determine the appropriate safeguards that may otherwise legitimize an international data transfer.

9. Sanctions

The high level of potential sanctions for breaches of the Regulation risks turning relations between companies and regulators into a combative one and may undermine the incentive of internet companies to invest in the EU.

The new proposal has a regime that includes very harsh fines for breaches of data protection law. These could be as high as 2% of the global revenue of a commercial enterprise.

Facebook is concerned that the magnitude of potential fines will create a disincentive for innovation and associated job creation among Internet service companies. This could be a major blow for the European Union given that the Internet sector is widely recognized as the major driver of job creation and growth; the 'Single Digital Market' concept the European Union is deploying recognizes this in many ways.

Moveover, it should be borne in mind that the level of potential sanctions might create a disincentive for open engagement by companies with regulators. Facebook's interaction with the Irish DPA and other regulators across the EU has shown that a lot can be achieved through open and transparent dialogue, even on difficult issues. A regime that threatens businesses with such heavy fines would imperil that cooperation and drive people away from an open relationship with DPAs. Ultimately this will not deliver privacy benefits as effectively as a less litigious model likely to be engendered by the proposed sanctions regimes.

10. Powers of the Commission to extend the Regulation

Proposals to grant the Commission wide-ranging powers to extend the Regulation should be considered carefully.

The Regulation includes 26 instances where the Commission has granted itself the power to extend the Regulation by adopting delegated acts in accordance with Article 86. Facebook is concerned that this approach might compromises the level of legal certainty afforded by the Regulation.

Facebook urges policy makers to ensure greater certainty by designing the process as transparently as possible and give the opportunity to the industry and other stakeholders to participate in it.

For further information please contact:

Erika Mann – Director of EU Affairs

Facebook Brussels

Rond Point Schuman 11 – 1040 Brussels – Belgium