Facebook Response to European Commission Communication on personal data protection in the European Union

Facebook welcomes the opportunity to comment on the European Commission Communication ‘A comprehensive approach on personal data protection in the European Union.’

This response has been prepared by representatives of Facebook Ireland Ltd and Facebook Inc. The lead author is Richard Allan, Director of Policy for Europe.

Background

Facebook provides a global social networking service that is used by many European citizens.

Facebook has a European headquarters in Dublin, Ireland and a subsidiary company, Facebook Ireland Ltd, which is the contracting party for all users of the service in Europe.

Facebook user data is stored in the United States on servers owned or managed by Facebook Inc. Facebook Inc has a comprehensive registration under the EU-US Safe Harbor scheme for its processing of data from European users.

Facebook users are provided with comprehensive information about the company’s privacy policies and practices on the Facebook site itself. This information can be found at www.facebook.com/privacy.

Detailed Response to the Commission’s Proposals

The Commission will consider how to ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals’ rights and freedoms and the objective of ensuring the free circulation of personal data within the internal market.

Because Facebook aims to offer a consistent service to all of its global user base, we welcome the recognition of the need for a coherent legal
framework that minimizes unnecessary burdens. The harmonisation of relevant data protection rules would assist in such an approach. In particular, further guidance to help businesses in establishing operations in the EU would be welcome.

The current EU rules on data protection aim to protect the fundamental right of the protection of personal data. Consistent with this objective, Facebook provides its users with industry leading controls over their data.

Facebook believes that by giving users tools to control their personal data, it is acting very much in alignment with the EU approach to data protection rights. This approach is supported by Facebook’s ‘Statement of Rights and Responsibilities,’ which includes provisions on personal data ownership and privacy rights. Facebook users have the ability to add, share or remove data however they choose, including to delete their entire accounts. Facebook users also have the choice to download their data, pictures, comments and full profile from the service.

Facebook supports the principle of transparency with respect to the processing of user data. We have great experience in this area as we have worked in the last six years to develop our privacy policy and our provision of privacy information to our users.

Facebook agrees that it is essential that individuals are well informed in a transparent way about how their personal data is being collected and used and how they can access and control their data, and Facebook aims to offer this high degree of transparency in its privacy policy. Facebook provides users with a clear and transparent guide through a ‘Privacy’ link on every
page, which helps users to control what data they share with the public, their friends, and other Facebook users, as well as applications and other websites. Facebook also provides clear and transparent explanations, both written and in video format, to educate users on their privacy settings.

We also recognize the need to ensure that younger users in particular have the information that they need to control their information on services like Facebook. To this end, we have developed a range of initiatives specifically targeting information to younger users.


We would offer a note of caution, however, on the proposal to require specific “modalities” for providing such information. Our experience has been that this is a rapidly developing field and that specifying such detailed requirements may not keep pace with innovation and therefore may not be effective. For example, because many of our users prefer instant messenger services to email services, a requirement to supply information by email would not reach many of them.

We would therefore suggest that the Commission instead set out the objectives it has in terms of the availability of and access to such information while remaining open to innovative approaches to the specific modes of provision.

We would offer a similar note of caution in respect to the proposal for “EU standard forms” for privacy information notices. While we understand the motivation for this proposal, there is a risk that it would run counter to innovative approaches by service providers and would risk making services inconsistent across different jurisdictions. In a world where online services are developing at a rapid rate in many diverse ways, requiring that such notices conform to a detailed standard might be insufficiently flexible to cater to a wide variety of circumstances.

We should also note that online services vary significantly in terms of the
data they collect, the features of the services and the design of their interfaces. This high degree of product differentiation helps to support a vibrant market in internet services to the benefit of consumers and will need to be taken into account in any standardization debate.

For example, we have developed an effective system for ensuring that Facebook users are asked to give specific permission to third party applications for the use of data. We believe that this innovative system places us in a leadership position in our industry. We are not confident that forms of notice mandated by regulations would be as effective as those which are already being developed by services such as ours.

The Commission will:
- examine the possible modalities for the introduction in the general legal framework of a **general personal data breach notification**, including the addressees of such notifications and the threshold beyond which the obligation to notify should apply.

Facebook welcomes the recognition that it is essential to look at the trigger criteria and methods of address when considering breach notification requirements.

Our primary concern in respect to such notifications is the potential for this to reduce rather than enhance user safety. This can happen in two ways.

First, if a regime subjects users to an excessive number of notifications, users may elect to ignore them, creating the risk that genuinely important and urgent information is missed against this background noise.

Second, any system of notifications from an online service about account security will be a target for hijack by those with malicious intent. Certain forms of breach notifications could inadvertently create a channel for those seeking illegal access to accounts. Systems must be designed so as to minimize these risks.
Facebook offers a service that is expressly designed for users to share personal data with a group of friends. The extent to which data is collected is therefore primarily a function of the decisions and actions of individual users rather than of Facebook itself.

Facebook reminds users in the ‘Statement of Rights and Responsibilities’ about their responsibilities in terms of posting data about others.

The user is able to exercise their subject access rights themselves by accessing their account and viewing, editing or deleting their personal data. This is entirely free of charge and can be done immediately. Where a user is no longer able to access their account and wishes to exercise subject access rights then they can contact us via our Help Center.

Facebook recognizes the value to users of data portability and has recently introduced a tool to allow its users to download a copy of their personal data from the service. This is a technically complex challenge given the rapidly evolving pace of development of services such as Facebook and because of the need to respect privacy settings for data that may have been uploaded by multiple individuals. We believe that we are providing an industry-leading portability service today and will continue to develop this service over time.

The explicit premise of the Facebook service is that when a user uploads data, it will remain available to the user unless and until he or she chooses
to delete it. The user is provided with tools to remove any individual item of data at any time. The user may also request that his or her full account be deleted at any time.

Facebook would be very concerned about any proposals that appeared to require the service provider to delete data without an explicit request from the user. Our ‘Statement of Rights and Responsibilities’ makes it very clear that user data remains the property of that user. It would run contrary to that notion of user ownership of data for Facebook as the service provider to delete it. Many people use Facebook as a long-term storage facility for archiving content like photos just as they may do with other cloud-based services and expect Facebook to keep this content available to them.

Our experience with our users is also that they use our service to build a record of their lives through the content they post. We have not been aware of there being a strong desire on the part of users for their data to expire over time. On the contrary, we believe that our users would be very upset if their data were to be deleted without their explicit approval.

We believe that any provisions in relation to the ‘right to be forgotten’ should be sensitive to the nature of each service. Services may differ widely. Some may be able to operate on the basis that data expiry is normal and storage extension is the exception as this reflects the nature of the service.

Others, such as ours, will be better able to serve the interests of our users by being able to give them the confidence that their data will be stored safely until they request deletion. Provided that they have effective deletion tools then this can meet both user and data protection requirements.

The Commission will explore:
- the possibility for co-financing awareness-raising activities on data protection via the Union budget;
- the need for and the opportunity of including in the legal framework an obligation to carry out awareness-raising activities in this area.
Facebook is supportive of expanding awareness-raising activities. We understand that these proposals are largely directed towards Data Protection Authorities who may be given new resources and obligations on awareness-raising.

As a private company we would be interested in exploring ways in which we can work in partnership with Data Protection Authorities on awareness-raising activities. We already work with a number of authorities and non-governmental organisations on similar activities and expect to expand this work over coming years. For example, we have provided extensive information to help the Norwegian Data Protection Authority to offer an advice service via their portal at www.slettmeg.no.

> The Commission will examine ways of clarifying and strengthening the rules on consent.

Facebook is an industry leader in offering its users effective controls over their use of data. We believe that this approach – providing sound controls for users within a service combined with full transparency in the terms of service and privacy policy – is an effective way of ensuring that there is consent for particular uses of data.

We also note that many of the operations carried out by our users are done so on a very regular basis which means that they are familiar with the consequences of particular actions they may make.

For example, over 50% of our users access the service every day suggesting that they have a high degree of familiarity with how it operates.

While we recognize the need to secure consent from our users and believe that we fully respect this in our own terms and operations, we wish to see a common-sense approach taken that recognizes the need to implement good service design.

For example, a consent model might be advanced that involves requesting individual consents for a range of items of data that are collected simultaneously. Such an approach could impose an unnecessary burden on users, as they already have sound knowledge of the product they requested
and the consents it needs.

There would be a high degree of user frustration if they were to be repeatedly asked for consents for something that is evident to them.

Facebook users will commonly share information that could be categorized as sensitive data such as their sexuality, religion and political views. It is entirely voluntary as to whether a user chooses to offer data for these items on their profiles. Whilst recognizing the importance of sensitive data, we would wish not to see any undue restrictions on such voluntary sharing.

We would ask the Commission to proceed cautiously with these proposals. Whilst there is no doubt that legal action is required in some serious cases, there is a risk that an excessively litigious environment would impede the development of innovative services that can bring real benefit to European citizens. The prospect of there being a wide range of bodies able to bring litigation against companies on data protection grounds may cause a great deal of uncertainty for businesses and significantly increase legal costs without evidence that there would be corresponding user benefits. We would ask that a thorough impact assessment be carried out of different options for enforcement.
Further harmonisation at EU level could help to increase legal certainty for businesses operating across the EU and therefore help to support the development of new services like Facebook.

Internet-based services in particular would benefit from simpler methods to ensure their compliance with the requirements of EU data protection law. It is common for an internet service to acquire users at a relatively early stage who live throughout the EU, even if the service has no or few local offices in member states.

It is unrealistic to expect such a service to have sufficient legal resources to be able to understand detailed data protection requirements across 27 different jurisdictions. If a service were able to test its compliance against a harmonized set of rules and be confident that it was then compliant across the EU then this would be an attractive option at an early stage of the development of a new service.

The benefits of such a simplification would assist services that originate within a single EU member state as well as those that are based outside the EU altogether.

The simplification of the notification system would be welcome as a way of reducing the administrative burden of compliance on business.
Improved legal certainty in the area of applicable law would be helpful. Such a process should recognize the realities of the development and growth of modern internet services such as Facebook.

Such services are typically developed in a single country and may gain an initial, substantial user base in that same country but will in most instances be accessible to users globally via the internet.

If such innovative businesses are to be able to develop, then the requirements for them to understand and comply with data protection law across multiple jurisdictions should not exceed their capacity to meet them.

The Commission will examine the following elements to enhance data controllers' responsibility:

- making the appointment of an independent Data Protection Officer mandatory and harmonising the rules related to their tasks and competences, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;
- including in the legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;
- further promoting the use of PETs and the possibilities for the concrete implementation of the concept of ‘Privacy by Design’.

Facebook understands that it has responsibilities as a data controller and strives to carry these out diligently.

We welcome the notion of an accountability principle and hope that progress will be made in creating routes for responsible companies to define a set of processes and safeguards against which they are willing to be held accountable. This type of process may potentially be more effective than a check-box approach to data protection compliance.

We would ask that any new requirements such as the appointment of Data Protection Officers and privacy impact assessments be considered in terms of their intended objectives and a degree of flexibility granted to organisations that have innovative approaches to achieving the same goals.
Facebook deploys a range of technological solutions that enhance the privacy of our users. We will continue to explore the best design and technology solutions to maintain our position as a leader in offering our users control over their data.

This is a rapidly evolving field so we remain cautious about any regulatory approach that would seek to specify particular solutions. We would be keen to explore further how encouragement can be given to organisations to deploy such design and technologies whilst also supporting continued innovation.

Facebook has been an active member of several self-regulatory initiatives, and we welcome future participation in existing initiatives, as well as the development of new initiatives. In particular, we are a signatory to the European Commission’s Safer Social Networking Principles and are represented on the Executive of the UK Council on Child Internet Safety (UKCCIS).

Facebook believes that self-regulatory initiatives by data controllers contribute to a better enforcement of data protection rules and are especially important in the rapidly moving industry of web services.

Facebook is already part of the TRUSTe Programme and awarded TRUSTe's Privacy Seal signifying that our privacy policy and practices have been reviewed by TRUSTe for compliance with their program requirements. Any such initiative in the EU should consider how global companies operate at scale and should consider recognising existing global schemes as having equal status with any locally developed schemes.
We understand that these proposals apply to the procedures of the various public agencies in the EU and therefore make no specific comment on them.

Facebook believes that the US-EU Safe Harbor scheme has a valuable role to play in this area. Facebook believes that this is an effective way to allow a US-based internet service to offer a high degree of protection to citizens across the EU during the time when it is developing services for EU residents.

The service may then move towards full EU compliance by creating an
establishment in one or more EU countries as Facebook has done by placing its European headquarters in Dublin.

Facebook joined the Safe Harbor scheme in 2007 and continues to maintain its certification. Full details can be found at http://safeharbor.export.gov/companyinfo.aspx?id=9633. Information about this registration is provided to users through its prominent inclusion in Facebook’s Privacy Policy.

---

The Commission will:
- continue to promote the development of high legal and technical standards of data protection in third countries and at international level;
- strive for the principle of reciprocity of protection in the international actions of the Union and in particular regarding the data subjects whose data are exported from the EU to third countries;
- enhance its cooperation, to this end, with third countries and international organisations, such as the OECD, the Council of Europe, the United Nations, and other regional organisations;
- closely follow up the development of international technical standards by standardisation organisations such as CEN and ISO, to ensure that they usefully complement the legal rules and to ensure operational and effective implementation of the key data protection requirements.

---

Facebook is an industry leader in providing technology that allows people to control the sharing of their personal data on the internet.

We work with a wide range of data protection regulators globally to ensure that we conform to the highest standards. We also have a strong track record of constructive engagement on privacy issues.
Facebook works with a number of Data Protection Authorities across the EU as well as with our primary Data Protection Authority in Ireland. We have also followed the work of the Article 29 Working Party with great interest.

Lack of consistency across member states does present a challenge for companies such as ours in seeking to offer a common service to all citizens in the EU.

The creation of local regulatory requirements in addition to the common ones that stem from the Data Protection Directive are a particular challenge.

The Commission will examine:

- how to strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities in the new legal framework, including the full implementation of the concept of ‘complete independence’;  
- ways to improve the cooperation and coordination between Data Protection Authorities;  
- how to ensure a more consistent application of EU data protection rules across the internal market. This may include strengthening the role of national data protection supervisors, better coordinating their work via the Article 29 Working Party (which should become a more transparent body), and/or creating a mechanism for ensuring consistency in the internal market under the authority of the European Commission.