



**Consumer
Focus**
Campaigning for a fair deal

Consumer Focus response to the European Commission's Communication on the 'Comprehensive approach on personal data protection in the European Union'

January 2011

ID: 55973692370-21

Introduction

Consumer Focus has worked and commented extensively on issues related to consumer privacy and data protection, both nationally and in the EU, including as members of the European Consumers Association, BEUC. We welcome this Communication as a further step towards ensuring a more effective and comprehensive regime for consumers' and citizens' privacy protection in the European Union. We are pleased that the Commission recognises the need to improve the coherence of the data protection legal framework in order to safeguard the fundamental right to privacy, as expressed both in the European Convention of Human Rights, and the EU Charter of Fundamental Rights.

We have always been strong supporters of the EU Data Protection Directive, and believe that its principles-based and technology-neutral approach and the principles themselves have been a success story and therefore must be maintained. We have, on the other hand criticised strongly the abysmal lack of compliance with data protection laws by data controllers and data processors, the inconsistencies between various national legislations, as well as the limited powers and weak enforcement by data protection authorities. We think that the application of the legal framework no longer adequately meets the challenges outlined in the Commission's Communication, such as the developments in technology and globalisation of data flows.

About us

Consumer Focus is the statutory consumer champion for England, Wales, Scotland and (for postal consumers) Northern Ireland. We were formed by the The Consumers, Estate Agents and Redress (CEAR) Act 2007.

We operate across the whole of the economy, persuading businesses, public services and policy makers to put consumers at the heart of what they do.

Consumer Focus tackles the issues that matter to consumers, and aims to give people a stronger voice. We don't just draw attention to problems – we work with consumers and with a range of organisations to champion creative solutions that make a difference to consumers' lives.

General remarks

Overall, the Communication reflects well the feedback from the series of stakeholder consultations, impact assessments and studies carried out in preparation to the review; it gives a fairly comprehensive picture of the new challenges to effective privacy protection; and on the whole it reflects well issues that will need to be addressed in the planned review of the data protection framework. The key objectives outlined are the right ones, though those connected to strengthening individual rights and improving enforcement must remain the absolute priorities.

However, in our view, there are areas that are not adequately addressed:

- Privacy enhancing technologies (PETs) and privacy by design is mentioned briefly in the context of enhancing data controllers' responsibility (2.2.4), but these are essential tools to ensure effective privacy protections that have been paid lip service in the past but little used. They should occupy a more important part in the review, including examining ways in which they can be practically adopted. For example in many online transactions it is not necessary to give away personal information and effective authentication technologies do exist. However they have not been widely adopted, or used, because it is rarely in the interest of online service providers to adopt or promote such technologies; their business models depend on constant personal data gathering, and this information has economic value. So there is an inherent tension between the rights of the individuals in legislation, and the desire of a great number of service providers to circumvent those rights as much as possible. These kinds of tensions will need to be addressed if a review of the legislation is to succeed
- While the need to enhance transparency is rightly acknowledged, there is no mention of the challenges posed by people's natural behaviour (as shown by behavioural economics research) and the need to address this within a future review. Any measure adopted in future legislation that will have data collection as default is bound to fail, as it has until now. So considerations of behavioural economics are particularly important in the context of discussions of various default settings and user control, as well as future risk/detriment assessments. Only privacy by default, data minimisation and avoiding unnecessary identification will go some way to meeting the stated goal of strengthening individuals' rights
- There is little mention of the challenge of dealing with the issue of individuals as data controllers – ie user generated content, bloggers, video makers that release a constant wave of personal data which is often public by default. This is a phenomenon that did not exist at the time of the formulation of the current directive, and needs to be addressed in any future review, since an individual using a platform service cannot be treated in law in the same way as a large service provider. In this respect we agree with the Article 29 Working Party, which recommends settings of maximum privacy by default on the platforms that provide services to individuals (blogging sites, social networks, etc)

We ask the Commission to address all these issues comprehensively during the coming process of the review of the legislation, in order to ensure a meaningful 'strengthening' of people's privacy rights. As the Communication acknowledges, the EU will need to have a consolidated general framework, which can be complemented with more specific rules and alternative measures. We give some more specific comments in the sections below, following the main headings and contents of the Communication.

Strengthening individual's rights

Ensuring appropriate protection

The Commission is right to address the concept of 'personal data', the issues round its definitions, and various processing and mining technologies as some of the most essential, if fundamental privacy rights are to be protected.

Regarding the definition of the concept of personal data, we support a wide definition, as included in the current Directive and interpreted by the Article 29 Working Party (Opinion 4/2007). This will continue to ensure the necessary flexibility and make the legislation future proof. The issue that will need to be addressed in the review is not the definition, but its different interpretations and lack of clarity on national levels, as is the case for example with IP addresses. One way to address this is to provide authoritative guidance that has to be taken on board by member countries, and the Article 29 Working Party is well placed to provide such guidance.

We also support consideration in the future review of additional Union law measures targeted at mining techniques and technologies, such as location data. The current debates in the UK round the implementation of the e-privacy directive with regards to user consent for storing of cookies in users' terminal equipment illustrate well the tensions between the service providers' desire to collect as much information as possible, and the need for data protection; if implementation is going to end up passing responsibility to individuals to set their own browsers at the appropriate cookie-rejecting levels, and/or possibility to opt-out via complex multiple choices on industry websites, then meaningful protection will not be ensured and the situation will be no different from the current one.

Increasing transparency for data subjects

We would support a general requirement for transparent processing, though after years of relatively fruitless discussions regarding simple or layered privacy notices and use of plain language, we are a little cynical on whether such a requirement can succeed in practice unless presentation and contents standards are also set by the data protection authorities. So we agree in principle with the idea of model 'privacy information notices' providing their design, placement and contents is brainstormed with stakeholders who understand behaviour economics, and user tested prior to release.

We are also wary of good transparency without meaningful choice, as happens now in many instances, where providers tell you comprehensively how they use your information, whom they share it with and how long they are going to keep it for, but you do not in fact have a choice, unless you reject the whole service, which means no choice at all in some cases. So while we strongly support transparency and easy, accessible privacy policies, we also urge the Commission to only consider this as part of a whole package of pro-privacy measures, as all too often transparency in itself is an easy 'win' and only measure. In general we also think that comprehensive privacy notices should be part of the consumer contract, for eg in contracts for energy or cloud computing services, and as such be subject to and comply with unfair contract terms legislation.

Regarding the statement on children in the context of transparency, we do not consider that good information alone is going to help much with the specific issues around the protection of children and minors. This is in fact the only place in the Communication where children are mentioned at all. We believe that more consideration should be given to privacy-related children's issues, such as classing their data as sensitive, and age verification methods.

Finally, and regarding transparency, Consumer Focus fully supports extending mandatory personal data breach notification from the telecommunication sector to all relevant industries and sectors (including public). We have been campaigning for such a measure to be introduced during the discussions on the revision of the e-Privacy Directive. We believe that extending the rule horizontally will ensure consistency between regulations, and will serve as a deterrent and incentive to companies to strengthen their security processes.

Enhancing control over one's own data

Consumer Focus would welcome an explicit reference to data minimisation in a revised directive as well as an explicit reference to, and clarification of, the right to be forgotten, which is particularly relevant in the context of social networking sites and cloud computing. However, we also believe that more effective in preventing future unnecessary data collection and profiling would be the introduction of the right not to be identified in the first place. There are many circumstances in which identification is not necessary at all for the provision of a service, and technologies are available that enable people to prove they are 'bona-fide' without the need to reveal personal information.

We support also looking at the ways that people's access, correction and deletion of personal information can be ensured without pain (for example through introduction of maximum response time limits and charge-free access) and looking at how to achieve better consistency in this respect between different member countries and data controller practices, which vary enormously at the moment, with the result that it is often very difficult for ordinary citizens to identify and correct errors.

Finally data portability is highly desirable, though it is a tall order to achieve it through data protection legislation alone – as essential prerequisites include software interoperability between various platforms, and open standards.

Raising awareness

While not averse to raising awareness, we are doubtful that such exercises can be successful unless they involve high cost strategic, targeted multi-media campaigns over a period of time and using social marketing techniques. Lessons should be learned, for example, from other socially-related issues, such as drinking and driving, and smoking awareness exercises. We suggest it would be more effective to target training and awareness raising campaigns at types of data controllers, and particularly small businesses or sole traders who increasingly monetise data without being aware of rights and obligations. As the Communication points out, a large proportion of EU data controllers have no knowledge of data protection legislation.

Ensuring informed and free consent

We agree with the analysis in the Communication regarding current Directive rules on consent (freely given, specific, informed) and consider that this is a fundamental issue to be resolved if data protection, especially online, is to have real teeth.

So we strongly support the intention to examine, strengthen and clarify the rules on consent, including ensuring much greater harmonisation between practices and interpretation in different countries. We ask the Commission to consider specific banning of unfair trading practices such as requiring consent as a condition of receiving goods and services, as well as introducing the concept of 'revocability', ie the possibility to take away consent previously given (similar to a 'cooling off period' available in online shopping or consumer credit contracts).

Protecting sensitive data

We believe that any data can become sensitive in certain circumstances and/or if linked to other available data; modern technology makes it possible to use information that is not considered sensitive under the terms of the current Directive for discriminatory purposes. So in an ideal world we consider that all personal information should be treated equally and have strongest protections. However, if current distinctions are retained, we would urge the Commission to add the following categories of personal information to the 'sensitive' list: genetic, biometric, family history, minors, financial data, and granular energy consumption data from smart meters (eg quarter or half-hourly live collections). This list should be made non-exhaustive to allow for future technological developments.

Making remedies and sanctions more effective

We strongly agree with the proposal to ensure more effective enforcement, including redress, as we see lack of implementation as the main weakness of the current data protection legal regime. Consumer Focus and other consumer and civil society organisations across Europe have been advocating for a long time the establishment of a judicial collective redress mechanism, both at national and European level, as an efficient tool for consumer empowerment and business compliance. This should include representative actions by authorities, consumer and other civil society associations on behalf of victims of data breaches, as well as collective redress.

We also support strengthened sanctions, but there should be a graduated range of sanctions commensurate with the seriousness of data breach, including criminal sanctions for the most serious mass breaches.

The internal market dimension

Increasing legal certainty and providing a level playing field for data controllers

Consumer Focus agrees that further harmonisation of national laws should take place given the cross-border nature of data flows, and not just European but generally global. However, we are concerned that further harmonisation does not result in reducing the protection of individual privacy to the level of the national legislations that are considered weaker overall, such as the UK. Examination of means to achieve further harmonisation of rules should have a clear preference for 'levelling up' to the highest common standards.

Reducing the administrative burden

We agree with the analysis in the Communication that the current system of notification should be simplified. Any such review should result in more coherent rules across member countries; the development of a 'model' notification should be considered.

We would not support however abolition of the notification system, as it can have an impact both on enforcement and transparency.

Clarifying the rules on applicable law and Member States' responsibility

We strongly agree with the expressed need to ensure the same degree of privacy protections of EU data subjects, regardless of the geographic location of the data controller, and therefore support review and clarification of existing provisions. We believe that if services are targeted at EU citizens, the law of the person's (data subject's) country of residence should apply.

Enhancing data controllers responsibility

We would support the introduction of a specific 'accountability principle' for both data controllers and data processors as appropriate, providing this is not a substitute for responsibility to comply with data protection legislation, but an additional obligation. Such obligation would mean that data controllers will have to demonstrate compliance with the legislation, and take appropriate measures to do so.

We would also urge the Commission to consider and clarify the roles and responsibilities of all those responsible for data processing, as in practice it is difficult for individual people to distinguish between a 'controller' and a 'processor', or a third party or a non-third party. Such relationships are increasingly complex, for example with the advent of cloud computing or in multi-national companies. Therefore we consider that data protection obligations and liability for breaches should be extended to data processors and third parties. This can also be achieved through specific contract terms, as it is now the case in other types of consumer contracts. So for example, social networking sites can be required to have contracts providing minimum standards of data protection when engaging third party service providers.

Regarding PETS and privacy by design, as mentioned in the general remarks above, we do not consider that the Communication gives these issues a fair hearing. We strongly believe that technical means and technological solutions can help people to be in control of their personal information and also help the enforcement efforts.

Therefore we urge the Commission to include privacy by design as an explicit and mandatory principle in any new framework for data protection. This would include both processes and technologies and give the necessary spurs both to ICT manufacturers and data controllers.

Encouraging self-regulatory initiatives and exploring EU certification schemes

We do not believe that self-regulation is the right approach in the field of data protection, and it is not compatible with the nature of data protection as a fundamental right in Europe. Furthermore, since the natural self-interest of service and goods providers is to gather and share as much data as possible, self-regulation without any firm controls for its effective implementation would be the equivalent of putting the wolf in charge of the sheep. A good example of this is the self-regulatory proposal in the field of behavioural advertising which is widely considered by consumer organisations and others as a poor response to privacy protection needs. We do however strongly support co-operation approaches, and forms of so-called co-regulation, for eg industry codes that clarify and support binding rules.

The global dimension of data protection

Clarifying and simplifying rules for international data transfers

We agree with the analysis that the assessments of whether data protection rules in third countries meet the EU standards (so called adequacy assessments) have not been satisfactory, and that the procedures need to be clarified and streamlined. The issue of export of EU consumer and citizen personal information to third countries is increasingly acute given the almost total globalisation of data flows, including expansion of cloud computing services and the extensive use of call centres outside the EU. At the same time experience with existing international agreements has not been so good, in particular we consider that the implementation of the EU-US Safe Harbour Agreement has been very poor. And as a matter of fact many companies based outside the EU but who do extensive business in the UK for example, such as search engines or major networking sites, claim that they are subject to their national laws, most often the US, which has a very different legal regime to that of the EU.

So we support the review of these provisions, and would urge that any future international agreements between the EU and third countries should reflect the high level of protection of privacy in the EU.

Promoting universal principles

We strongly support the continuation of a leading role for the EU in promoting strong international data protection standards. We also believe in the need to develop universal principles and global standards. We particularly ask the Commission to support and actively contribute to the current revision of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal data, as an opportunity to ensure greater convergence with the EU framework and enhanced protection for individuals.

Stronger institutional arrangement for better enforcement

We have been campaigning for a long time for enhanced powers for the Information Commissioner in the UK, and therefore welcome the intention in the Communication to both strengthen the roles of the Data Protection Authorities (DPA), and the co-operation between them. We ask for greater harmonisation of standards for DPAs powers and particularly for their independence both material and in terms of whom they answer to. We believe they should be answerable to Parliament rather than particular government policy departments. This would ensure both greater transparency and accountability to the public at large.

We also support enhancing the role of Article 29 Working Party as a means to ensuring greater consistency within the EU. In particular its Opinions should take the form of Guidance to be adopted both in the Commission proposals and by DPAs on national levels. Further, Consumer Focus believes that the consumer protection authorities and other regulators have a role to play as additional enforcers, as privacy is a cross-cutting issue. Poor data protection practices can effectively be considered as unfair commercial practices, and in fact in many sectors, such as energy, privacy terms and conditions are a clause in the wider contract with consumers.

Conclusions/way forward

We support the proposed next steps and look forward to discussions and co-operation with the Commission, the Parliament and the Council on the detail of the proposed framework during the course of 2011.



Consumer Focus response to the European Commission's Communication on the 'Comprehensive approach on personal data protection in the European Union'

If you have any questions or would like further information about our response please contact Marzena Kisielowska-Lipman, Senior Policy Advocate, by telephone on 020 7799 7981 or via email: marzena.kisielowska-lipman@consumerfocus.org.uk

www.consumerfocus.org.uk

Copyright: Consumer Focus

Published: January 2011

If you require this publication in Braille, large print or on audio CD please contact us.

For the deaf, hard of hearing or speech impaired, contact Consumer Focus via Text Relay:

From a textphone, call 18001 020 7799 7900

From a telephone, call 18002 020 7799 7900

Consumer Focus

4th Floor
Artillery House
Artillery Row
London SW1P 1RT

Tel: 020 7799 7900

Fax: 020 7799 7901

Media Team: 020 7799 8004 / 8005 / 8006