Internationale Politikanalyse
International Policy Analysis

European Integration Working Group*

# Civil Rights, Security and Consumer Protection in the EU

## Civil Liberties: Data protection as a cornerstone of European domestic policies

■ In view of increased criminal use of the internet, the state must obtain the instruments required for exchanging data and surveillance of communication. At EU level, increased data exchange is already required because of the Schengen Area.

■ The legitimacy of both European and national measures is, however, only guaranteed if the extended availability of personal data is reasonably proportionate to freedom of personality, protection of the private sphere and one's informational self-determination. To this end, strict conditions must be imposed.

■ In the EU, with the Treaty of Lisbon, data protection will finally receive fundamental right status. In the sphere of police and judicial cooperation in the EU, an attempt has been made to strengthen data protection with a corresponding framework decision. Many provisions are, however, imprecise and leave it to the discretion of the national authorities to define the limits for forwarding and use of person-related data.

■ In addition to the use of data by public authorities, misuse of data in the private sector is an increasing problem. Data retention generates an additional problem of trust at the interface between prerogative use of data and commercial data storage. For use of customer and user data in the private sector, stronger boundaries must be drawn and penal measures provided for in the event of violation.

JUNE 2009

FRIEDRICH EBERT STIFTUNG

## Content

## 1 Introduction

In the past few years, the European public has been shocked more and more frequently by data protection scandals, which in some cases were caused by errors made by public institutions (Great Britain), and in others by downright criminal misuse of employee and customer data in companies (Germany). These scandals accompanied and discredited various legislative initiatives – both at member state and EU level – which extend the capabilities of the police and the judiciary to access data about citizens and which are intended to improve data exchange between police authorities. At the same time, the aims of these legislative projects, fighting criminality and terrorism, are also an absolutely accepted concern among the wider public. Yet to what extent do these measures endanger the private sphere and the fundamental rights of citizens?

## 2 Security and civil liberties in the EU

The debate about the limits of state access to internet and communication data was ignited, particularly in Germany, by the debate on data retention, whereby the German interior minister had already greatly contributed to uncertainty among the population with his demands for extended online search capabilities. It is indisputable that in an increasingly technically advanced and globalised world, the police and investigating authorities are more reliant than ever on data exchange and communication via the internet or other networks. With a view to the increased use of the internet for criminal schemes and the enormous increase in crimes committed on the internet, the state must also obtain the necessary instruments to be able to adequately protect people online. According to a forsa survey, more than 4 million Germans have already been victims of internet crime, most of them having suffered financial loss due to phishing, credit card swindles or virus attacks.

At EU level, the necessity for increased data exchange already exists because of the Schengen area. In an area of open borders and merging economic areas, there are boundless fields of activity for organised crime. National police authorities and isolated search databases alone will not be able to cope with this internationalisation of crime. The Schengen information system (SIS), Europol, the Visa Information System (VIS), the querying of DNA data (Prüm Decision) in addition to data retention, provide some responses to this problem. Yet the legitimacy of these measures is only then guaranteed if the extended availability of personal data is reasonably proportional to freedom of personality, protection of the private sphere and one's informational self-determination.

Therefore, the following conditions must be met for all measures comprising storage, processing or forwarding of personal data:

1. Personal data is recorded only for a clearly defined and limited purpose. The scope and application of the recorded data must be proportional in view of the purpose of the measure and the extent of the curtailment of personal rights. The proportionality must be shown comprehensively.
2. The storage, processing and forwarding of data must promise real progress for specific crime fighting measures and be absolutely necessary for investigative work. The necessity and proportionality of the intervention must be regularly checked by the legislator.
3. The party affected must be able to inspect the data stored and delete any erroneous information.
4. Data security must always be guaranteed.
5. Data may only be forwarded to other agencies or to third countries if the data protection level is as high as in the EU.
6. It must be legally guaranteed that the data stored cannot be used for measures other than those intended (so-called data mining). Any other or extended use of existing databases may only occur with a new legal basis. Possible database tapping through the backdoor – comitology procedures, ministerial orders – must be ruled out.

Requirements for the justification of necessity and proportionality must be included, from the beginning, in legislative initiatives and proposals tabled by government representatives. All too often it has been the case that, because of media reporting, Ministers and Commissioners have announced new monitoring measures which have proven to be neither suitable nor to conform with basic law. The former EU Commissioner, Frattini, thus caused considerable upset by announcing a series of initia-

* The European Integration Working Group of the EU Office of the FES in Brussels has been in operation for more than ten years. Its members include experts from the European institutions, German federal ministries and regional administrations, organisations and the scientific community.

tives such as monitoring of entry and exit travel and of maritime borders or a European system of air passengers' data recording. At the same time, the benefit of such systems for the security of citizens is gravely in doubt. In Great Britain, where a pilot project for air passengers' data recording is currently in progress, to date it has been mainly illegal immigrants who have become the »victims« of these measures. There has been no advance in terms of fighting serious crime or terrorist activities. Before the population is alarmed by the announcement of new interventions into the private sphere, from the very beginning, high requirements concerning justification of curtailment of fundamental rights should be placed on initiatives tabled by the European Commission and national ministries.

## 3 Fundamental right of data protection

In the European Union, with the coming into effect of the Lisbon Treaty, data protection has now finally been accorded fundamental right status, since the protection of personal data is confirmed by Article 8 of the Charter of Fundamental Rights. In the area of the internal market, data protection is regulated by directive 95/46/EG which, particularly thanks to the setting up of the group known as the article 29 data protection group, has made a considerable contribution to improving data protection at EU level. Like the European Data Protection Supervisor, this independent committee evaluates all EU measures concerning the personal data of EU citizens and thus influences the legislative initiatives of the European Commission and the debates of the European Parliament.

The third pillar of EU responsibilities in the area of police and judicial co-operation (PJC) was for a long time missing a framework for data protection. Indeed, the individual measures each include specific data protection regulations, yet there was a lack of basic regulations for storing, processing and forwarding data as part of a criminal prosecution. The framework resolution concerning data protection in the area of PJC was finally passed by the Council of Ministers last year, after more than three years of negotiations. It has, however, been criticized by data protection campaigners for various reasons. Many provisions are very imprecise and leave prerogative of interpretation concerning forwarding and use of person-related data to national authorities. In addition, the forwarding of data to third counties must be more strongly restricted. This point was already of vital significance during the debate about forwarding air passenger data (so-called PNR-data) to the USA, since here sensitive personal data about EU citizens is regularly transferred to a third country for up to 15 years. Citizens must be able to rely on the fact that such processes respect their private sphere and that there is adequate legal protection. In the case of the agreement with the USA, there is considerable doubt. Moreover, the forwarding of bank data of European citizens to American authorities through the SWIFT company, shows that within the framework of transatlantic dialogue, the EU should resist such greediness more strongly. Protection of the fundamental rights of people in Europe must have priority over friendly diplomatic turns. Data must only be requested and forwarded on the basis of perfect procedures according to the rule of law, with respect to the procedural laws of those concerned.

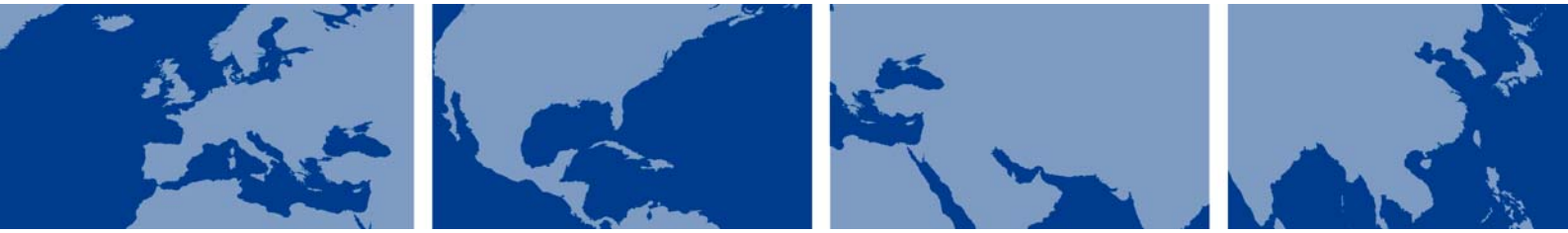
## 4 The private sector: Data protection is consumer protection

But it is not only with police co-operation that there are shortcomings in the area of data protection. Many data protection problems that have emerged over the past few months have occured in the private sector and particularly in companies. The security of employee and customer data must, therefore, be re-evaluated and regulated more restrictively throughout Europe. Likewise there must be a stronger focus on protection of the private sphere in the internet. This includes the question of the extent to which providers and other types of suppliers are allowed to use customer and user data for commercial purposes and where the boundaries are to be drawn (see Telekom, Microsoft, Google, Facebook). If the European Parliament and the Council of the European Union gain agreement in the Conciliation Committee for the telecom package, some improvements in data protection within the framework of electronic communication are to be expected. The extent to which further concrete measures will be necessary depends on the final result of negotiations.

The problem of using customer data at telecommunication groups and internet providers has acquired a new perspective in terms of data retention. In order not to subject the state, and particularly the police, to the suspicion that they wish to systematically record all spheres of life of the popu-

lation, the relevant directive envisages storing data with private service providers. Only on the strength of a judicial writ, can the law enforcement authorities gain access to the data. According to the law, the retained data should be saved separately from other firm data and must not be used by the companies – but the data protection scandals of the past few years leave grave doubts as to whether this instruction is being followed in practice. Owing to the size of the problem, this risk of misuse must be re-evaluated at European level. Alternative solutions should be sought – in case of doubt, data retention must be dispensed with. In any case, the member states are requested to stipulate criminal measures in the event of serious violations of internal data protection. Financial sanctions alone – even when they amount to millions, as in the case of Lidl – do not seem a great enough deterrent when faced with the magnitude of the problem.

Finally, thought should also be given to measures protecting online users against unintentional disclosure of personal data. For data protection breeches on the internet is frequently necessitated by the non-reflective and non-uniform behaviour of users and not solely by data protection leaks in companies. Private information is thus placed in public areas of social networks or other platforms, under the assumption that these are only available to a limited number of people. It will not be possible to counteract this development through information campaigns only. Measures on the side of the provider will also be required to advise users of this. Because for both new and unpractised users, the internet must not become a risk to their private sphere.



Imprint
Friedrich-Ebert-Stiftung
International Policy Analysis
Division for International Dialogue
D-10785 Berlin

www.fes.de/ipa
E-Mail: info.ipa@fes.de

ISBN: 978-3-86872-124-9

Orders
Friedrich-Ebert-Stiftung
International Policy Analysis
Nora Neye
D-10785 Berlin

E-Mail: info.ipa@fes.de
Fax: +49 (30) 26935-9248

All texts are available online:
www.fes.de/ipa