February 2011

AK Position Paper

# Opinion on the Communication from the Commission on the comprehensive approach on personal data protection in the European Union

www.akeuropa.eu

# About us

**The Federal Chamber of Labour is by law representing the interests of about 3.2 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore the Austrian Federal Chamber of Labour is a part of the Austrian social partnership.**

**The AK EUROPA office in Brussels was established in 1991 to bring forward the interests of all its members directly vis-à-vis the European Institutions.**

**Organisation and Tasks of the Austrian Federal Chamber of Labour**

The Austrian Federal Chamber of Labour is the umbrella organisation of the nine regional Chambers of Labour in Austria, which have together the statutory mandate to represent the interests of their members.

The Chambers of Labour provide their members a broad range of services, including for instance advice on matters of labour law, consumer rights, social insurance and educational matters.

More than three quarters of the 2 million member-consultations carried out each year concern labour-, social insurance- and insolvency law. Furthermore the Austrian Federal Chamber of Labour makes use of its vested right to state its opinion in the legislation process of the European Union and in Austria in order to shape the interests of the employees and consumers towards the legislator.

All Austrian employees are subject to compulsory membership. The member fee is determined by law and is amounting to 0.5% of the members' gross wages or salaries (up to the social security payroll tax cap maximum). 560.000 - amongst others unemployed, persons on maternity (paternity) leave, community- and military service - of the 3.2 million members are exempt from subscription payment, but are entitled to all services provided by the Austrian Federal Chambers of Labour.

Herbert Tumpel
President

Werner Muhm
Director

# The AK position in detail

The development of the protection of fundamental rights in Europe is a particular concern for the Federal Chamber of Labour (AK).

The development of the protection of fundamental rights in Europe is a particular concern for the Federal Chamber of Labour (AK). While it welcomes the various efforts of the EU Commission to promote the completion of the internal market, it also strongly advocates the needs of consumers and workers to be sufficiently taken into account.

Against this background, the AK is pleased to have the opportunity to comment on the Communication from the Commission on plans in the data protection area:

**Review of the Communication in regard to those concerns, which AK referred to the Commission in 2009**

In 2009, during the consultation on the community legal framework concerning the fundamental right to protection of personal data, the AK had expressed an opinion on the necessary amendments to the General Data Protection Directive 95/46/EC adopted 15 years ago.

In particular, it highlighted that in addition to the necessary update of the general provisions, there was an urgent need for sectorspecific provisions in those areas of life, in which complex IT applications have gained on importance in recent years, and where there are serious conflicts of interest in the society with regard to the confidentiality of data or its use.

**Sufficiently specific, binding rules are lacking for example,**

1. for the use of **new privacy-sensitive technologies** (web services, RFID, biometrics, location based services, video surveillance, etc.).

2. in those areas of life in which the possibilities and interests to use personal data have massively increased, but because of the **power imbalance between the originator and persons affected by the process, declarations of consent do not** in general provide an appropriate legal basis:

2.a **Data protection in the employment relationship**

One of the areas which needs to be regulated is the use of data by employers. Given that the free will of employees in the employment relationship tends to be largely reduced, a voluntary consent cannot be presumed. More generally, it is apparent that the particularly sensitive area of employment relations, typically characterised by an imbalance of power requires special protection.

In practice, it would be very important to provide for a mandatory appointment of a Data Protection Officer, who would ensure the legal use of data– in particular employee data – within companies. The fact that the employers' knowledge and thus their regulatory compliance is surprisingly low has been demonstrated repeatedly both in practice and in surveys.

The authorisation to represent or serve the interests in data protection matters before the authorities should be extended – in any event, employee representatives (works councils) should be able to carry out this role on a company level.

It would be very important to provide for a mandatory appointment of a Data Protection Officer

In practice, domestic companies transfer data to their foreign parents, which has proven to be a recurring problem – additional enforcement and sanction mechanisms are needed here to be able to act across borders in case of infringements.

2.b **Data and consumer protection**

In other situations of everyday legal life, there are also significant doubts about the voluntary nature of the consents granted, which is why preference should be given to a sector-specific provision of the directive clearly limiting the use of data: Companies increasingly refuse to conclude agreements with consumers if they are not prepared to consent to **data use provisions for marketing, credit check or scoring purposes.**

**In its opinion from 2009, the AK has suggested, among other things, the following changes to the General Data Protection Directive in order to bring it up to date with the current protection requirements of the parties concerned:**

- Introduce a disclosure requirement of the originator in relation to the parties affected or the national data protection supervisory authority in cases of serious privacy violations **(data breach notification)**
- Stricter formal requirements for consent declarations
- Clarification of the **laws applicable** to data protection infringements on websites (laws in the place of residence of the consumer who uses the website)
- Obligation of the originator to undergo privacy audits (PIA - Privacy Impact Assessment, e.g. award of the EuroPriSe - European Privacy Seal) and submit these to the registration authorities prior to processing intrusive data.
- Request for information from the personal data user, in principle, on all source data, not only (as it is currently the case) on data, which is still "available" (logging obligation)

**We expressly welcome the fact that**

- the extension of the **data breach notification** to cover areas, which do not fall in the scope of application of the e-Privacy Directive is being considered.

- the Commission will examine ways of clarifying and strengthening the rules on consent

**Stricter requirements for declarations of consent** are a central concern for the BAC:

We expressly that the extension of the data breach notification to cover areas, which do not fall in the scope of application of the e-Privacy Directive is being considered.

In the commercial sector, data is increasingly used based on the agreement of the parties concerned, especially for marketing purposes. Under current legislation, consents are only effective if they are given freely with full knowledge of the facts and thus the implications of the decision.

In practice, individuals often overlook consent declarations, which tend to be hidden in the text of terms and conditions or do not get to see the underlying contract clauses at all, as it is the case when the contract is concluded over the phone. The burden of proof for the validity of the consent lies with the user of the data. However, affected individuals tend to notice illegal data use due to missing, hidden or nontransparent consent declarations only at a very late stage - when data has already been sold and households are being harassed by unsolicited telephone advertising.

Against this background, it should be specified what the requirements are with regard to clarity and form for the obtained consent declarations to be effective.

1. Consent clauses **must be clearly highlighted and separated from the remainder of the text of the contract thus making them easily recognizable.**

2. In principle, **consents must be granted in writing** (implied consent regarding the acceptance of terms and conditions should be inadmissible).

3. A consent can also be granted effectively in an electronic form when the user has to make an active step (for example, by ticking a box), the consent is logged and the user can access its contents and revoke it with effect for the future at any time. If the consent cannot be easily revoked (for example, the website no longer exists), all the consents granted to date are deemed to have been revoked.

- the Commission will consider introducing a general **principle of transparent processing,** the provision of information in relation to children and drawing up EU **standard "privacy information notices" forms.**

Under Article 2 of the Directive 95/46/EC, an effective consent declaration is based on "informed consent" on the part of the data subject, in other words,

on a sufficient explanation about the content and purpose of data processing, any recipients of disclosed data, etc. Article 11 of the Directive also points out that the originator has to inform the individuals concerned "fairly". The welcome intention of the Commission to create greater transparency also implies that in addition to the existing general principles, sufficiently precise guidelines should be developed to provide basic information on standard situations (participation in social networks, consent to use data for own or third-party marketing purposes, consent to process and share credit scoring data). Under these circumstances, EU standard forms "privacy information notices" in areas that suffer from a particular lack of transparency would be greatly appreciated.

The AK believes that the issue of applicable data protection legislation should be regulated in a more consumerfriendly fashion.

- the Commission will examine how to revise and clarify the existing provisions on **applicable law:**

Since many consumer activities are shifting toward the Internet and international offers can thus be accessed very easily, the AK believes that the issue of applicable data protection legislation should be regulated in a more consumerfriendly fashion than has been the case so far. This issue is particularly pressing when the data processor is established outside of the EU and does not comply with EU data protection standards. The legal point of reference used to date (the use of technical facilities located in a Member State) has not proven itself in practice. In the absence of access to internal company information, it is neither possible nor reasonable to expect individuals to do this research. We support the opinion of the Article 29 Working Party (wpdocs 2002/wp56), according to which the technical operation of placing cookies on a user's personal computer should be considered performed in the place of residence of the affected user. The general application of data protection legislation at the place of residence of the internet user would build on similar arrangements in the field of consumer law and would be an important measure reducing the legal protection hurdles for internet users.

- the Commission will examine the measures to enhance data controllers' responsibility, in particular, by introducing the obligation to appoint an independent **data protection officer or to carry out a data protection impact assessment** in certain cases and promoting the use of privacy enhancing technologies (privacy-by-design):

- **Data protection officer** The Europe-wide introduction of a data protection officer would be an extremely important step towards a more effective enforcement of data protection rules in the workplace. Given the rapid pace of technological progress (e.g., in standard software alone) the demands on employers and employees are increasing. There is, therefore, a very urgent need to provide for a data protection officer, who ensures enforcement of data protection rules at a company level.

In principle, the disclosure obligation should extend to all source data and not only to data, which is still "available" (as it is the case at present).

Based on the German model of the Federal Data Protection Act, the data protection officer in a private company (or in the public sector) would have to ensure compliance with data protection regulations and in particular, advise management on all relevant data protection matters, monitor data security measures (such as issuing and controlling access rights to databases), ensure that data subjects can exercise their rights to information, rectification and deletion and to train staff in relation to data protection. Data protection officers must be independent and autonomous in their office and should not be subjected to any disadvantage as a result of performing their duties.

- **Mandatory audits:** Similar to the official inspection of a completed building project after submission of a civil engineering evaluation or a vehicle inspection to ensure compliance with statutory standard values, the data controllers should be subject to (regular) privacy audits by independent assessment bodies at least in the case of intrusive data (e.g. sensitive data) or the use of data, which is difficult to verify (internet services).

In this way, data protection compliance should be broadly ensured. Data protection supervisory authorities cannot realistically fulfil this supervisory function given the millions of registered data applications. They rely on complaints. Since data processing is increasingly less visible and perceptible by consumers and takes place "behind the scenes," the enforcement of data protection legislation cannot rely solely on privacy complaints. It would be high time to establish a preventive system of scrutiny. We consider the EU certification project EuroPriSe to be exemplary in this regard. In the absence of a mandatory audit, the number of certified data applications is disproportionately low, compared with the total number of intrusive data processing operations in Europe.

The Communication of the Commission did **not address** the demand for a broadly unrestricted request for information from the data processor. In principle, the disclosure obligation should extend to all source data and not only to data, which is still "available" (as it is the case at present).

For explanation: The information as **to the source** of data under the Directive 95/46/EC should only be issued when this information is **still available.** If processors want to disguise the source of dubious data, they report that the data is no longer available. The proposed solution: it should be always possible to query the source of data (exception: the processor can prove why logging the data source would present a disproportionate burden and the lack of information does not adversely affect the data subject in enforcing his right to deletion, etc.).

Information should also be provided on **"recipients or categories of recipients"** of data. When it is sufficient to specify the recipient only as a sector (e.g. banks, insurance companies, credit agencies, etc.) and when a specific

company must be disclosed, is often a point of contention. Proposed solution: the actual recipient should always be disclosed.

**With regard to the privacy on the Internet, the AK has suggested the following priorities in its opinion from 2009:**

- Disabling of automatic search engine hits on web sites
- Data protection requirements for the terms of use of social networks
- "Right to be forgotten" or the right of the individuals to have their self-generated internet entries no longer processed and deleted (forum posts, communication on social networking sites, etc.)
- Determining personal data deletion rights for externally generated entries, e.g. search engines and websites
- More straightforward consent forms for the use of cookies (alternatives to complicated privacy policies that are difficult to understand for consumers); addressing the massive enforcement deficit for the inappropriate use of cookies (covert use, data use for other than the designated purpose, excessive storage time, unauthorised disclosure of data to third parties)

We expressly welcome the fact that the Commission will examine ways of strengthening the principle of data minimisation, improving the enforceability of individual rights and clarifying the socalled "right to be forgotten".

**We expressly welcome the fact that**

- the Commission will examine ways of strengthening the principle of data minimisation, improving the enforceability of individual rights and clarifying the socalled "right to be forgotten".

The issue has become particularly virulent because of possibilities for the use of personal data on the internet. Once the data is legitimately publicly accessible, its protection cannot be adequately guaranteed. Given the size of the data published on the Internet, this principle now appears obsolete.

Everyone, whether a blogger or a participant in a chat or discussion forum or an online community leaves personal information behind. It has now become common practice to "google" a name if you want to learn something about a person (e.g. a job applicant). While internet comments and forum posts, which often contain personal information are directed primarily at a defined circle of friends or acquaintances, it can ultimately be accessed by anyone. Any use of this data for marketing purposes, copying to other websites, creation of web search profiles, the use of data long after it had been deleted from the original website, etc. should not be justified by the fact that the data is available on a website. The fact that personal data is held at a location, which is freely accessible,

should not lead to the conclusion that the subject's data is no longer protected and thus can be reused in any other possible context and disclosed without limitation. In particular, there should be limits for the sale of data while recognising that the published personal data should also be subject to some degree of confidentiality protection. In practice, personal data for profiling on the internet is intensively searched, analysed and sold. If the restrictions on use would be more clearly defined on websites, it is highly unlikely that commercial data use would be authorised.

In practice, personal data for profiling on the internet is intensively searched, analysed and sold.

The EU Data Protection Directive does not indicate in any way that the individual's privacy, once the data has been legitimately published should no longer enjoy any protection. However, clear protection standards are missing.

**Confidentiality interests deserving protection should therefore be considered violated when the reuse of publicly available data is not consistent with its original purpose.**

**Further adaptation requirement:**

Currently, Web 2.0 users need to rely on the goodwill of the providers even for the simplest data protection measures. Web 2.0 users should retain control over the published data on the internet. They should, for example, have the right to

- let **selfgenerated content expire at a specified date.** Internet users complain, in our view rightly, that posts that remain available on the internet for many years, present an outdated image of the individual without a clear and easily enforceable entitlement to a removal after a certain period of time has passed.

- **make search engine hits subject to the express consent of the data subject.**

In this context, also common problems with **internet search engines** should be clearly addressed:

- people search engines should not use internet entries of individuals without their express consent (see the strict requirements of the Article 29 Working Party on search engines WP 148/2008).

- service providers that invite users to publish their own contributions should be required to offer an opt-out feature from search engine indexing.

- the request from affected individuals who do not want to be subjected to search engine indexing with respect to their web content (by using the Robots Exclusion Standard, for example), would have to be respected by search engine operators.

We welcome that the Commission will examine further harmonisation steps at the EU level.

As a result of the Communication, the strengthening of the principle of data minimisation is also being considered. The Communication stresses that limitation of processing for a specific purpose is the precondition for a high level of data protection. We refer in this regard to the broad constitutional criticism of the **Directive on data retention for telephone and internet communication.** The storage of personal data of millions of customers without reason for possible future use in law enforcement (for a longer period than necessary for billing purposes) is contrary to the above described principle: the purpose has to be clearly defined already at the time of processing. Because the enormous amount of data can hardly be suitable for fighting terrorism and represents a severe violation of privacy rights of the customer contrary to Article 8 of the European Convention on Human Rights (ECHR), the revision of the Directive should be included in the priority privacy projects of the Commission.

**Furthermore, we welcome that the Commission will examine further harmonisation steps at the EU level.**

The Communication rightly emphasizes that there is a need for harmonisation in many sectors and contexts and reference is made to the use of data in the employment context or for public health purposes.

**From AK's point of view, the following sectorspecific rules are urgently needed:**

- Protection for the use of customer data, especially imposing limits for scoring methods
- scope and limits of the (international) trade of customer data,
- more stringent requirements for the consent for the use of data for marketing purposes
- limits on the use of credit scoring data, especially considering automated calculation of scoring values
- consideration of data protection standards for law enforcement treaties, which contain highly sensitive personal data – such as the SWIFT Treaty.
- **Data protection for new technologies**

Location based services (location based data such as navigation services, Google Street View, etc.):

Increasingly, user location data but also images of buildings and land are being collected. These services use geographic coordinates to determine a location and to assign an exact building address to a resident. Against this background it should be made clear

- that location data may be used only for the provision of services, which have been actively ordered by the user. The consent for the use of data must be given by the user separately and expressly.

- that the identification and retrieval of georeferenced and systematically available images should only be authorised, if it does not override the legitimate interests of data subjects. In assessing the interests which warrant protection, the purpose of use should also be taken into account along with pontential transmissions and the type of access.

- that it is absolutely not authorised to display faces or vehicle registration numbers.

- that the opportunity to object exists before the provision of appropriate information to the public.

**Radio Frequency identification**

The very specific recommendations of the European Commission (Recommendation of 12 May 2009 C (2009) 3200 final on the Privacy and Data Protection Impact Assessment Framework for RFID Applications) directed at the controllers of RFID-enhanced data applications should be binding.

**Video surveillance**

In many Member States, for example video data is not considered sensitive, although Article 8 of the Directive 95/46/EC could also be interpreted in such a way that every video recording contains sensitive data, because it can be used to draw conclusions on health or ethnic or religious affinity of individuals. Harmonisation would therefore be appropriate.

**In principle, we also welcome the proposals of the Commission to make remedies and sanctions more effective, including extending the power to bring an action before the national courts to associations and strengthening the existing provisions on sanctions:**

In principle, we also welcome the proposals of the Commission to make remedies and sanctions more effective, including extending the power to bring an action before the national courts to associations and strengthening the existing provisions on sanctions.

The resources of the individual data protection supervisory authorities are very limited. Therefore, it is hardly feasible to take on supervisory responsibilities covering all the relevant fields in addition to dealing with individual complaints. Taking into account the enormous number of data applications, the enforcement deficit would hardly decrease, even if more personnel and increased funds could be channelled towards it. **In order to bring the Directive up to date with the conditions of the 21st century, it should shift to preventive data protection through certification, funded by the processor,** which should be more than a mere registration. If data protection is to be taken seriously, it should involve – as previously described - mandatory audits, at least for intrusive data applications (similar to vehicle registration and regular inspections). The implementation can be assigned to a variety of accredited bodies (such as IT specialists

and lawyers with the necessary technical and legal expertise).

As to the announcement by the Commission that it intends to examine opportunities for simplification and harmonization of the notification procedures, including the introduction of a uniform EU-registration form it should be noted that:

Easy access to information of those concerned, who the processor is in relation to which data and data disclosure, must remain unrestricted.

It is true that the individual data protection authorities are stretched to their limits by the sheer number of notifications. In the absence of detailed examination of the legal compliance, the register does not signal the admissibility of the notified data applications at present. But at least it fulfils an important publicity role: anyone can obtain information about notified data applications. Easy access to information of those concerned, who the processor is in relation to which data and data disclosure, must remain unrestricted. A departure from the registration obligation would only be possible if it were replaced by an effective alternative system in the form of a data protection officer at a company level. Simplification of the registration rules can therefore, only be agreed to if the transparency of processing is ensured by other means (an obligation to appoint a data protection officer who will maintain transparent specifications) and the current regulatory enforcement deficits are removed by "outsourcing" preliminary examinations (processor funded audit opinions or certifications by independent bodies, etc.).

The AK is therefore pleased that the Commission has entitled one of the chapters **"More responsibility to the data processor".** In contrast to administrative simplification, the **principle of accountability should be** considered.

We expressly welcome this plan of the Commission. However, the sentence "the possible introduction of an accountability principle" would not aim to "increase the administrative burden on data processors" has given rise to considerable scepticism. Merely promoting voluntary selfregulation (as described in section 2.2.5) in return for simplified reporting would not be an adequate response. The undergoing of audits, award of certification and the implementation of "Privacy by Design" at company level (technology "with built in data protection") is in any case an additional (at least financial) burden for the economy. If the plan should lead to serious improvements, it needs clear legal obligations. Their enforcement against the expected resistance of the economy certainly represents a challenge for the Commission. Nevertheless, we consider certification requirements (at least with regard to sensitive technologies, processes, products or services, which should be defined) to be absolutely timely and without a real alternative.

**Furthermore, we welcome that the Commission will examine the inclusion of the areas of police and judicial cooperation in criminal matters in the Data Protection Directive:**

The provisions in different legal instruments in the area of the former First and Third pillar of the EU were implemented for legal reasons relating to competency. These have been abolished with the entry into force of the Lisbon Treaty. A comprehensive data protection regime, including the police and judicial cooperation in criminal matters would be absolutely justified (considering some logical constraints such as the disclosure or information obligation).

Furthermore, we welcome that the Commission will examine strengthening of data protection authorities and the cooperation between them:

**Furthermore, we welcome that the Commission will examine strengthening of data protection authorities and the cooperation between them:**

The need to help to reduce the burden of the individual data protection authorities and the options available such as mandatory, privately funded audits have already been mentioned several times.

Moreover, the role of Article 29 Data Protection Working Party should be enhanced. The independent Article 29 Data Protection Party has been so far responsible for the interpretation of the Directive. It made valuable contributions in the past - many of which had been ignored in practice. The "checklists" for a variety of privacy related areas it creates with a great effort and expertise should form the basis for future mandatory certification procedures.

Should you have any further questions please do not hesitate to contact

**Daniela Zimmer**
T: +43 (0) 1 501 65 2722
daniela.zimmer@akwien.at

as well as

**Christof Cesnovar**
(in our Brussels Office)
T +32 (0) 2 230 62 54
christof.cesnovar@akeuropa.eu

**Bundesarbeitskammer Österreich**
Prinz-Eugen-Strasse, 20-22
A-1040 Vienna, Austria
T +43 (0) 1 501 65-0
F +43 (0) 1 501 65-0

**AK EUROPA**
Permanent Representation of Austria to the EU
Avenue de Cortenbergh, 30
B-1040 Brussels, Belgium
T +32 (0) 2 230 62 54
F +32 (0) 2 230 29 73