February 2013

AK Position Paper

Position paper on the draft report on the 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)

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, communityand 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 future development of consumer and employee-related data protection in Europe is an issue of particular interest to the Federal Chamber of Labour (BAK). It welcomes the efforts to promote free movement of data within Europe, yet it also emphatically advocates that regulations must take sufficient consideration of the needs of consumers and employees. Against this background, the BAK fully appreciates the opportunity to present its opinion on the amendments to the draft report by the Committee on Civil Liberties, Justice and Home Affairs:

1. Positioning on the EU Commission's draft for a General Data Protection Regulation from the perspective of consumer policy and employees:

The BAK supports the EU Commission in its efforts to establish up-to-date, harmonised data protection at the highest level. **Several of the proposals taken up by the Commission's draft are in agreement with consumer demands that BAK has highlighted for a number of years.**

We would particularly like to emphasise that, in addition to the amendments necessary for bringing the general conditions of the current RL 95/46/EC up to date, there is an urgent need for sector specific regulations in areas of life in which, over recent years, complex IT applications have been introduced and sharp conflicts of interest have arisen socially regarding the confidentiality of data and its use. **Specific, binding regulations are somewhat lacking**

1. for the use of **new, data protection-sensitive technology** (Internet services such as apps, RFID, biometrics, geo-based services, etc).

2. for those areas of life where the possibilities and interest in the application of personal data have increased massively. Yet due to the **particular imbalance of power** between employers and the processing of declarations of consent from data subjects, often no appropriate legal basis is available: this certainly includes the use of data from **employees by their employers**. The free will of those affected in the work relationship (and in the application process) has generally depreciated to such an extent that voluntary consent cannot generally be assumed.

And in other situations of contractual everyday life there are also general doubts about the free will of the consent that has been given, which is why sector specific standards that explicitly limit data use are needed: for instance companies increasingly deny consumers contractual agreements unless they give consent to data sharing clauses relating to **marketing, credit assessment and scoring purposes**.

The BAK regrets that in comparison to unofficial preliminary drafts **the Commission's official draft has decreased consumer protection levels**. Thereby, in the event that their data is used for **direct marketing purposes,** consumers should be entitled to a right of withdrawal – **originally instead of**

opt-outs there were opt-ins, in other words a requirement for explicit consent was intended. Considering the diverse range of target group specific marketing activities on the Internet, which are based on consumers' personal data without their knowledge, this represents a disappointing lower level of protection from a consumer point of view. In addition, possible sanctions for breaching regulations have been reduced.

Moreover, many good regulative ideas end just in hopeful headings, with effective content not being reflected in the provisions. In other words: in many cases due to vague specifications it remains unclear to what extent the proposal actually represents an improvement to the current situation. The minimum requirements from the BAK's perspective are that the provisions in the regulation must under no circumstances fall short of the current legal situation in Member States. To illustrate this point, the duty of employers to implement an **impact assessment** is very welcome, as employers will be more accountable for their data processing.

However, clear specifications are lakking as to under what circumstances such an impact assessment is to be implemented, to what extent, whether employers or data protection authorities decide if the content will also be subsequently checked, who has access to the results, etc.

Against this background, we fear that this measure presents no improvement, but rather the opposite - a considerable step backwards (with the simultaneous dispensing of the current management of a data processing register). By means of specific processing rules, authority controls and publicity of the data applications used, at the minimum both transparency and legal certainty should be achieved in this respect.

We reject the proposal for a one-stop-shop process, whereby in the future only the data protection authority in the Member State where a company has its headquarters shall be responsible in the event that data processing is carried out transnationally. Employees and consumers have a heightened need for protection – as for instance the provisions show regarding the proper place of jurisdiction for this group of people (the possibility to lodge a complaint at the place of execution or place of residence must be stated). Therefore it appears not to be appropriate to refer to a data protection authority abroad. The reduction of a company's administrative costs should not lead to a deterioration of the legal protection for consumers and employees (similarly the proposed concept of the leading authority in Amendment 277 (Article 54a) cannot fully dispel these concerns).

It is of note with regard to corporate data protection that there is an employee limit of 500 staff members after which a corporate data protection officer is to be appointed. This is set much too high (the limit of 250 employees contained in the original Commission's draft was criticised by the BAK for being too high), e.g. for Germany this regulation would mean a massive deterioration in protection. Data protection is a basic right (the emphasis of this assessment in the amended draft is welcomed greatly by the BAK), to which employees in small and medium-sized businesses are also entitled. Furthermore, stricter regulations are required for commissioning,

dismissing and appointing data protection officers (thus perhaps a right of participation of the works council would be desirable as there should be an explicit, embedded termination and discrimination prohibition in place for data protection officers in order to strengthen their independence).

Regarding the amendments:

2. The BAK's concerns regarding the following amendments:

- **Amendment 8 Recital 15 and correspondingly Amendment 79 Article 2 paragraph 2 d**

Recital concern: „With the personal use of electronic services a distinction must be made between communication with a certain group of recipients and publication of personal data to a non-specific extraordinarily large number of recipients. In the latter case, those involved must be able to exercise their rights, in particular to delete and correct.

Justification:

The exception from the scope of application of the regulation for exclusively personal or family activities goes too far: The EU Data Protection Regulation should not only differentiate between commercial activities (for gainful interest) and private purposes, but rather should also consider other factors (such as the effects of a (partial) publication of data on the Internet). In cases of data use in social networks it should be ensured that those involved are entitled to certain conditions of approval rights, at least correction and deletion rights.

The applicable EU Data Protection Directive 95/46/EC already allows exceptions from the data protection provisions in favour of the use of data for exclusively private purposes. This approach from 1995 corresponds to the common private „household" requirements (for example, taking a child's birthday, private contact database, etc.) yet not the requirements for use of the Internet. Problems with classifications, which private activities should and should not fall expediently within the areas of exception, are posed above all with regard to online activity in social networks. For instance, users use social media platforms not only to exclusively refer to themselves but also to report on friends, their jobs, etc. The question remains open as to what extent in general (or only depending on the individually selected privacy settings on the platform) such activities which (partially) publicly disclose information about third parties should be subject to the „household" privilege.

There are actually protection requirements on both sides: firstly those individuals involved who do not wish to disclose personal data under the circumstances to a larger group of people without their consent. On the other hand, it must be acknowledged that the idea of privacy amongst the younger generations of „digital natives" has changed significantly. The communication of information to a Facebook group of 100 friends is viewed by many users as being the equivalent to talking in a private group of regulars at the local bar.

- **Amendment 26 Recital 41 and corresponding to Amendment 101 Article 6 paragraph 1b new**

Concern: Deletion of the exception from the requirement of consent for „certain associations or foundations"

Justification:

An exception from the obligation to receive explicit consent, in favour of „legitimate activities by certain associa-

tions and foundations" is not factually justified. Fundamentally it privileges fundraising associations to enable them to contact potential donors. Given that telephone marketing, for example, based on purchased consumers' address data is a great nuisance and the group of beneficiaries can also include untrustworthy providers, the exception should be completely deleted.

- **Amendment 35 Recital 54 and correspondingly Amendment 147 Article 17 paragraph 2**

Concerns about combining the Commission's draft and the amendment proposal: the duty of data controllers to communicate the request for deletion by data subjects to all the data recipients (Commission proposal) should be combined with the task of the data controller to take all necessary steps to have the data deleted by recipients (Amendment).

Justification:

The Amendment proposal is supported by the BAK. Yet often it is impossible in practice for data controllers to delete data from all possible third parties (for instance copies of countless websites). Therefore data controllers should at least be obligated to inform third parties about the consumer's request for all data to be deleted.

- **Amendment 37 Recital 57**

Amendment concern: If personal data is used for direct marketing purposes, prior, explicit consent from the data subject should be required.

Justification:

The Commission proposal to benefit direct marketing for non-commercial purposes through an opt-out (Recital 57) is rejected as is the general privilege for direct marketing in Article 19 paragraph 2. Direct marketing in particular via the Internet has taken exceptionally non-transparent and unlawful forms.

Against this background it is therefore important to reinforce the position of consumers by means of a right of consent for use of personal data for direct marketing purposes (instead of a mere right to withdraw).

- **Amendment 58 Recital 97 and corresponding Article 51 paragraph 2 Jurisdiction**

Amendment concern: „If individuals are affected by suspected violations by a company in more than one Member State (e.g. as consumers, employees), they should be able to appeal to the data protection authority in their country of residence. If proceedings on the same grounds as the complaint have already been initiated in one Member State, appealing to another data protection authority may temporarily suspend the proceedings. The leading data protection authority must coordinate with the other authorities concerned. If legal questions are disputed between the authorities involved, they should appeal to the EUGH."

Justification:

The one-stop-shop-principle is rejected: the location of the headquarters of a company should not establish the

exclusive responsibility of a data protection authority. The proposal would mean that appropriate authorities for an Austrian subsidiary of an international group would no longer be the Austrian data protection authority but the authority at the place of the group's principal establishment. Thereby in the event of a violation, access to the law by works councils, data protection officers and consumers in a country with a number of subsidiaries is impeded. Groups of companies (from third party countries) could additionally operate forum shopping, in other words they could choose the location of their headquarters in the country with the weakest law enforcement.

As such there are few doubts that affiliated groups such as Facebook would choose the location of their headquarters (in this case, Ireland) on the basis of location advantages which could be detrimental to those involved. Although data subjects could still turn to their national authorities as a contact point, these would not have any decision-making powers if the opponent maintains its headquarters elsewhere. The reduction of administrative costs and requirements at companies must not lead to detrimental legal protection for consumers.

- **Missing Amendment to Article 3 - geographical scope of application of the regulation**

Without corresponding implementation agreements with other countries, such as the USA, it is a well-intentioned but difficult standard to enforce in practice.

Justification:

The expansion of the geographical scope of application to other countries is welcomed wholeheartedly. Currently one of the biggest problems is the lack of enforceability of data protection laws against large multinational companies that are not established in the European Union. In order to enable effective legal enforceability in practice (for example against social networks based in the USA), mutual law enforcement agreements would be required and the European Parliament should work to achieve this.

- **Missing amendments to Article 7 in connection with Article 6 paragraph 1b new and Article 19 - overriding legitimate interests in direct marketing for their own or similar products; consent and withdrawal**

Concerns: deletion of Art 6 para 1 b point c) and Article 9 para 2 with a new paragraph in Article 7 instead:

„The requirement of prior, explicit consent by the data subject is especially applicable to data processing for direct marketing purposes.

Consent given for marketing purposes is forfeited at the latest at the end of the contractual relationship, in other cases two years after the consent has been provided.

If consent has been obtained via a written data protection clause, the types of data must be clearly and transparently stated, along with the

processing purpose, the maximum retention period and the purpose and potential recipients. It must also emphasise the right to withdraw consent at any time and the consequences for data subjects. Moreover, it must clearly state which data is compulsory for the purposes of fulfilling the contract and which information is voluntary."

Justification:

It is indeed welcomed that consent must be given explicitly in the future (as silent acceptance of terms and conditions, for instance, is no longer sufficient). Yet this must be equally applicable to the use of consumer data for direct marketing (a lowering of the level of protection to a mere withdrawal notice and the right to withdrawal is not acceptable from a consumer perspective).

In particular, in cases of contracts with consumers, the privilege to be able to use direct marketing to sell its own additional products or similar products is wholly disproportionate (Amendment 101 to Article 6 para 1b new). In this situation, it is not just the case that no consent (opt-in) would be required, but there is also no requirement for the company to inform the consumer openly about the use of data and the existence of a right of withdrawal. This would be a considerable step backwards compared to the current legal position (opt-out). It must also be considered that this includes nuisance forms of advertising, such as marketing calls and mail shots.

A maximum time frame for the applicability of authorised consent would be desirable as consumers can no longer remember years later that they - allegedly - once gave their consent to use their data for marketing purposes. Subsequently data should be deleted or consent must be re-authorised.

In order for data subjects to evaluate the consequences of this decision prior to giving their consent, they must be informed about the scope and purpose of the data processing. The definition in Article 4 refers to this as „with full knowledge of the facts". Minimum requirements are missing from the content of a data protection clause in Art 7.

- **Missing Amendment of Article 8 Processing of personal data of a child**

Concern: deletion of „information society services".

Justification:

It is indeed welcomed that children are especially protected as a result of the provision. However, it is not comprehensible as to why the protection is limited to the use of online services („information society services") and furthermore why the same regulations should not apply to consent from minors.

In addition, further detailed regulations are lacking, such as when and to what extent minors between 14 and 18 can independently give consent and exercise their rights as data subjects.

Furthermore, it must be ensured that the verification of age limits by online service providers does not give cause for non-required age verification and additional data gathering which can be used for other purposes (such as marketing).

- **Missing amendment to direct marketing Article 19 para 2**

Concern: Deletion of paragraph 2

Justification:

As we have stressed on a number of occasions, the BAK regrets that the requirement for consent is not (any longer) included for the use and sharing of data for direct marketing purposes. In Austria (requirements in the Commercial Code) only restricted data may be transferred from businesses to direct marketing companies without authorised consent, therefore this proposal would represent a step backwards. If this regulation is implemented, consumers would forfeit their in practice already barely enforceable ability to independently control the use of their data. Empowered consumers want to decide themselves which data they release and to whom they make data available. Against this background, the exceptions from the requirement for consent should be omitted without substitution.

- **Missing amendment to Article 20 para 3 - Measures based on profiling**

Amendment request: „Credit rating data and profiling processes should only be allowed to be used in the framework of agreeing contracts in which there is evidence of particular default risks.

For the prognosis of default risks, only factually relevant credit rating personal data, such as payment problems and insolvency data, may be used (Note: no discrimination using „soft" data which can be interpreted in a number of ways; no past incidents from many years ago, no involvement of statistical data which are appropriate only under certain circumstances).

If scoring methods are used they must lead to scientifically-valid results (and be approved and regularly reviewed by independent authorities)

The suppliers and buyers of credit rating data must work transparently. Consumers should be informed about the data used, the use of scoring methods, etc. (Note: this is the only way that allows data subjects to effectively oppose questionable methods.)

Credit rating data must be up-to-date and correct (Note: older data pools are to be deleted due to a lack of validity concerning an individual's current credit rating).

Health-related data may not be used for credit scoring.

Justification:

There is an equally poor overview available with regard to the types of data used as is the case with when and where consumers can be classified. The German credit protection organisation Schufa discloses that the *„number and type of credit activities, possible default on payments or related information, and how long you have accumulated experiences dealing with credit companies."* are used in the calculation of a credit score. The following aspects are not included: *„We have no information regarding nationality, profession, income, family status or about which residential area you live in."*

However, what is seen as voluntary self-limitation, can also only be a division of tasks in individual cases: Often inquiring companies (insurance company, mail-order company, mobile phone provider, etc.) only request raw data from a credit agency and then supplement this with data that appears on a contract application or from socio-demographic static population details, etc. The score is then calculated by the mail-order company itself, for example.

There are problematic aspects in this regard: as a result of the various buyer - service provider relationships it is difficult for data subjects to know where data is saved, what is statistically enriched and what will be used for the assessment.

As there is a lack of specific rules of practice, there is a risk that it will often be the case that incorrect characteristics, or false or out-of-date data will be processed and „hard" and „soft" facts will be mixed.

Score models are the best kept trade secret

One person - one score value? Whether someone will pay back a home loan or will pay a mail-order company invoice on time are questions that can be based on various risks. Many companies therefore apply their individual processes. One can look in vain for publicly available information about the assessment methods - in terms of selection and weighting of parameters. Credit agencies refer to it as a trade secret.

It is a core business and a competitive advantage over competitors to improve the validity of prognoses by means of ongoing review and feedback from users. Lack of transparency leads to data subjects being unable to find any simple defence against the use of doubtful methods, for example.

Improvements would bring about a general duty of disclosure of methods (e.g. in published terms and conditions) and certification by a scientific institute.

- **Amendment 176 Article 23 Data protection by design and by default**

Recital request: The supplier of services made available free of charge must also provide anonymous (pseudonym) user options.

Justification:

Unless required for billing purposes, users should not be obliged to register with their actual names. The reference to Article 5 para 1a new is welcomed (device features and online services that can transfer personal data going beyond what is required for pure contract fulfilment. For instance, location data for apps and marketing data for social networks must have factory default presets so that they best meet the confidentiality interests of the user.)

- **Missing amendment to Article 33 Data protection impact assessment**

Redesign: Member States must maintain a data protection register. Data protection impact assessment and data protection officers are the only conceivable alternatives, insofar as they are regulated thoroughly.

Justification:

Currently there is a lack of clear legal obligations: who decides when about

the existing mandatory auditing of processing risks? Who warns or forces data controller audits to be carried out (if there is no longer any data protection register providing information about high-risk data applications)? Who should implement audits? Who controls and safeguards, if necessary, the results and conclusions? Should the results be published? In the event of a delay, can the data protection authorities commission an audit at the location and at the expense of the data controller?

The resources of the individual data protection authorities are so limited that it is hardly possible to deal with matters beyond individual complaints, let alone systematically looking after the supervisory tasks of all relevant areas. In view of the gigantic number of data applications, implementation shortfalls would scarcely be reduced even through the use of a considerably larger number of personnel and funds. The cornerstone of a regulation could therefore be a move to preventive data protection through certification financed by applicants. Given that the auditor in the model of Article 33 is also the inspector, a wealth of detailed guidelines and supervisory measures are required to ensure that the standard is effective in practice. The statement by the EU Commission triggered considerable scepticism, „the possible introduction of the accountability principle" should lead „to no additional administrative costs for the applicant ordering the processing". The mere promotion of voluntary self-regulation in return for the full reporting requirements in store would in no way be adequate for the problem.

The carrying out of impact assessments in the form of audits, the acquisition of quality certificates and the implementation of „privacy by design" within the company presents in any case an additional (at least financial) burden for the economy. If the provision is to bring serious improvements, it requires clearer legal obligations, controls and sanctions, which are missing in the draft. The implementation must be assigned to specially accredited bodies (IT specialists and lawyers with the necessary technical and legal expertise).

- **Amendment 223 Article 35 para 1b Designation of the data protection officer**

Concern: deletion of Amendment 223

Justification:

The obligation to appoint an operational data protection office only after a company has 250 employees was already set too high in the Commission's proposal (for instance, in Germany the obligation to appoint a data protection officer applies from a significantly lower threshold). In any case it would be desirable for the employee threshold to be set considerably lower (for example, from 20 employees). It would be conceivable to adjust it based on additional criteria, beyond the number of employees, such as the sensitivity of the data processing or the number of data subjects. However, it should be clarified that on exceeding even one of the criteria the appointment of a data protection officer is required.

- **Missing amendment to Article 40 - Transferring of personal data to other countries**

Comparable regulations in the RL 95/46/EC have in practice not really been proven. Indeed there are few

provisions to ensure that countries without equivalent data protection levels act diligently with received or transferred data. For example the „Safe Harbor Agreement" with the USA has not contributed in any great way to ensuring that the legal protection of consumers is sufficiently safeguarded when transferring consumer data such as flight passenger details for purposes of domestic security.

- **Amendment 313 – Article 77 Right to compensation and liability**

Amendment concern: flat-rate compensation would be desirable - also for immaterial damages – combined with a reversal of the burden of proof in favour of the consumer.

Justification:

Following illegal use of personal data, the injured party would no longer have to establish an exact amount of damages, but rather only if this exceeded the flat-rate sum.

- **Sanctions (Article 78, Article 79)**

The BAK regrets that the maximum sanction limit has been lowered compared to the unofficial drafts. Originally, the highest penalty was up to 5 percent of the annual profit worldwide.

The fact that penalties for wrongdoing must also be appropriate, in other words minor offences can naturally also only be tackled with minor penalties, is derived in any case from the administrative procedure regulations.

- **Amendment 43, 50 and 60 – inclusion of the works council**

In a corporate context, the importance of including the occupational interest representation (the works council) should not be overlooked.

Therefore, it appears to be useful to also make reference to the works council in the course of the documentation provisions in Amendment 43, which must also have the opportunity to verify the employer's use of data. Similarly, a reference to the works council would be desirable among the institutions entitled to appeal (Amendment 60), as it represents the interests of the employed workers – who typically don't have enough confidence in the existing employment relationship to assert a claim themselves. As far as Amendment 50 makes reference to codes of conduct, it should be noted that the use of works agreements concluded between employers and workforce representation for purposes of data protection of employees should also at least be mentioned.

3. The following amendments have our full support:

- **Amendment 12 Recital 20 and correspondingly Amendment 82 Article 3 para 2 a**

This is a significant clarification that employers from other countries are also subject to the EU data protection regulation if they offer products and services to European consumers free of charge (for example, financed by advertising).

- **Amendment 13 Recital 21 and correspondingly Amendment 84 Article 4 No. 1**

This is an important increase in the protection level that, except for the observation of user behaviour on the Internet, any data collection from European consumers by companies based outside of the EU is subject to the EU data protection regulations.

- **Amendment 15 Recital 24**

This is a significant clarification that user recognition, such as IP addresses, SIM card identification, inter alia, fall under personal data generally worthy of protection (unless it is proven – quasi within the framework of the burden of proof – that it is a company identification that does not enable any conclusions regarding an individual).

- **Amendment 17 Recital 31**

This is an important emphasis that consent must satisfy certain requirements - namely being given „explicitly" and „with full knowledge".

- **Amendment 19 Recital 33**

This is an important increase in the protection level whereby *„default presets are used that individuals must change themselves, in contrast to the use of default pre-checked boxes that do not express free consent*" (Note: this clarification is so significant in practice, due to the many violations, that it should also be included in Article 7 Consent).

- **Amendment 20 Recital 34**

This provides an enormous increase in the level of protection, whereby *„the processors of data that have considerable market power*" under the circumstances mentioned in the amendment cannot use consent from consumers as a legal basis for data processing, as the consumers are in a similar dependent relationship as is now the undisputed case with regard to the relationship between employees and to their employers.

- **Amendment 22 Recital 38**

This is an important increase in the level of protection as the general catch-all provision „of prevailing legitimate interests" may only be used as a legal basis in exceptional cases and data subjects can also object to use of data without stating any reasons.

- **Amendment 24 Recital 39 a new**

This places a considerable restriction on data use options as data cannot be gathered from people as a preventative measure for the implementation of legal claims or for safeguarding against payment defaults, but rather only with regard to consumers where a contractual legal right has already existed for data collection.

- **Amendment 25 Recital 39 b new**

This is a significant increase in the level of protection offered, as using data for purposes that do not correspond

to the primary reason for storing the data is forbidden. In other words, the secondary use of data also requires its own legal basis.

- **Amendment 36 Recital 55**

This is a significant clarification, that a claim for „receipt of his or her personal data" can be exercised free of charge.

- **Amendment 39 Recital 59**

This is an important improvement, as exceptions to the rights of data subjects in favour of public security, inter alia, are acceptable, but cannot be used with regard to „important scientific or financial interests of Member States". With this far-reaching exception there could be justified encroachments on data protection which totally undermine the rights of the individuals concerned. The public interest in controlling the correctness of taxes and contributions paid, for example, could be subsumed under the prevention and detection of criminal offences.

- **Amendment 41 Recital 61 and correspondingly Article 5 para 1a new**

This is quite a crucial improvement whereby services and devices have data protection-friendly default presettings. This is the only way to ensure that smartphones, for example, do not regularly transmit location data to app manufacturers or that Facebook users do not unintentionally make their information available beyond their friends to the entire world.

The average consumer is overwhelmed by service and device preset options. The obligation for providers to give a strict „factory" default setting is absolutely correct in this age.

- **Amendment 55 Recital 92**

This is an important comment whereby data protection authorities must have adequate financial and personnel resources. The implementation of data protection regulations in a complex and rapidly changing technological environment has often been wantonly neglected in the past.

- **Amendment 66 Recital 114 and Amendment 310 to Article 73**

This is a significant extension, whereby in cases of data protection violations not only data protection organisations but also other institutions authorised to deal with complaints such as employee and consumer protection organisations, trade unions, etc., can support those involved.

- **Amendment 100 Article 6 para 1 a new**

This is a significant improvement, whereby data controllers (unless it involves an authority) that base the permissibility of data processing on the very imprecise legal basis of „legitimate prevailing interests" must inform data subjects regarding the processing and the reason for processing „explicitly and separately". This approach is a better way than was the case in the past for ensuring that data subjects actually find out about the processing and for ensuring that, if necessary (asserted overriding confidentiality interests), they can exercise their rights.

- **Amendment 102 Article 6 para1 c new**

This is a significant improvement, whereby in a list of examples it is noted when confidentiality interests prevail (e.g. location data, biometrics, profiles, publications, data from children).

- **Amendment 107 Article 7 para 4 b new**

This is a considerable improvement, as a „prohibition on coupling" is incorporated at this point: according to this, the use of a service must not be made dependent on requiring consent from consumers to use their data for other purposes other than providing the service.

- **Amendment 124 Article 13**

This is a significant improvement, whereby the Commission draft states that data controllers must inform data recipients of a request for deletion from data subjects and as a result of the amendment, data subjects must be informed of the names of any recipients.

- **Amendment 164 Article 20 para 2 b new**

This is an important clarification, whereby creating behaviour profiles of minors is prohibited.

Amendments that restrict the intended legislative powers of the EU Commission in 26 articles with regard to implementation methods of the regulation:
In order to ensure a careful separation of powers between legislative and executive, all amendments that aim to restrict the EU Commission's power to pass delegated acts are welcomed.

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

Gerda Heilegger
T: + 43 (0) 1 501 65 2724
gerda.heilegger@akwien.at

and

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