DER HESSISCHE DATENSCHUTZBEAUFTRAGTE
als Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2015

14. August 2015

Conference of the Data Protection Commissioners
of the Federal Government and the Federal States (Länder)

Key data protection points for the trilogue on the General Data Protection Regulation

I. Preliminary remarks

After the Justice and Home Affairs Council adopted its position on the General Data Protection Regulation on 15 June 2015, since late June the European Commission, Parliament and Council have been discussing their positions on the Regulation in what is known as the trilogue, with the aim of reaching an overall agreement and adopting the legally relevant act by the end of 2015.

Since the Commission presented its proposals in January 2012, the conference of Germany's data protection commissioners of the Federation and of the Länder has repeatedly made public its position on data protection reform. It presented its opinion on the entire package on 11 June 2012 and on individual aspects of the data protection reform in a series of resolutions and opinions.[1] From the beginning, the conference supported the Commission's aim of building "a modern, strong, consistent and comprehensive data protection framework for the European Union",[2] all the more so as the Commission explicitly focused on individuals' fundamental right to privacy, which the reform is intended to serve.

[1] Resolutions *Ein hohes Datenschutzniveau für ganz Europa* (A high level of data protection for all of Europe), 21–22 March 2012 and opinion of 11 June 2012; *Europäische Datenschutzreform konstruktiv und zügig voranbringen!* (Advancing European data protection reform constructively and quickly), 8–9 November 2012; *Europa muss den Datenschutz stärken* (Europe must strengthen data protection) and explanations, 13–14 March 2013; *Zur Struktur der Europäischen Datenschutzaufsicht* (On the structure of European data protection oversight), 27–28 March 2014; and *Datenschutz-Grundverordnung darf keine Mogelpackung werden!* (The General Data Protection Regulation must not become a fraud), 18–19 March 2015, all available in German at www.bfdi.bund.de/DE/Infothek/Entschliessungen/DSBundLaender/Functions/DSK_table.html.

[2] "Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century", Communication from the Commission, COM(2012) 9 final, no. 6.

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telefon (06 11) 14 08-0 · Telefax (06 11) 14 08-9 00 oder -9 01
E-Mail poststelle@datenschutz.hessen.de · Internet http://www.datenschutz.hessen.de

This is why it is extraordinarily important for the conference of federal and state data protection commissioners that the General Data Protection Regulation should ensure better or at least the same level of protection of fundamental rights as current law, which is largely determined by Directive 95/46/EC. The reform of European data protection law must absolutely not result in a lower level of data protection than is currently in place. The conference emphasizes that the fundamental principles of data protection based on Article 8 of the EU Charter of Fundamental Rights and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) should therefore not be open to discussion. There are still no specific requirements governing high-risk data processing, such as profiling or with regard to video surveillance. And the Regulation still allows data to be processed for advertising purposes without the data subjects' consent. Precisely in this era of Big Data and global data processing, the autonomy of the individual, the transparency and lawfulness of data processing, purpose limitation and the accountability of controllers are just as important for safeguarding fundamental rights as strong supervision of data protection and effective sanctions.

These issues and others addressed in the following are the most important points which the conference of federal and state data protection commissioners believe the participants in the trilogue should especially concentrate on.

For ease of use, this paper is oriented on the structure of the current drafts of the General Data Protection Regulation.

II. The individual proposals

1. The scope of the General Data Protection Regulation

a. The household exemption must not be expanded!

The Council has expanded the household exemption in Article 2(2)(d) of the Regulation by crossing out the words "without any gainful interest" and "exclusively" in the Commission's proposal.

The Council's proposal is formulated in a way that would exempt a substantial part of the processing of personal data by natural persons from the scope of data protection law even if the fundamental data protection rights of third parties were significantly infringed upon. As formulated by the Council, even if the processing for personal or household purposes represented only a minor purpose when considering the whole, it would still fall under the household exemption and would therefore no longer be subject to data protection law. Users of a social network or operators of a private website would be exempt from the law, even if they

published large amounts of personal data without restriction on the Internet, as long as they declared they were doing so (also) for personal or household purposes. Such expansion would be unacceptable. Nor can the intention to make a profit serve as a criterion for applying data protection law, because the degree to which data processing interferes in privacy does not depend on the profit motive. Expanding the household exemption too far would conflict with the fundamental right to privacy guaranteed by primary law and therefore cannot be implemented in secondary law.

The conference opposes expanding the household exemption in Article 2(2)(d) of the General Data Protection Regulation and the resulting limits on the scope of data protection law. The household exemption should therefore continue to be oriented on the wording of Article 2(2) of Directive 95/46/EC and only exempt processing related exclusively to personal and household activities.

b. The scope of the Regulation must not be further restricted in favour of the proposed Directive on data processing by the police and judicial authorities!

The Regulation will not apply wherever the Directive (see COM(2012)10 final) applies. In this way, the scope of the Directive also determines the scope of the Regulation. With this in mind, the Council has discussed various proposals in recent months, some of which could lead to a significantly expanded scope for the Directive.

The conference sees no convincing reasons to depart from the division between the Regulation and the Directive as originally planned. According to the Commission's original proposal, the Directive lays down rules relating to the "protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties". The Council has objected that this does not include threat prevention where it is intended to prevent a crime, which in turn means that data processing by the police would be subject to two different legislative acts. In order for all police tasks to be governed by a single act, i.e., the Directive, the Council believes that the scope of the Directive should be expanded accordingly. There has even been talk of including data processing by the public order administration in the Directive.

The conference of federal and state data protection commissioners opposes such expansion. If a compromise must be found which expands the scope of the Directive for data processing by the police, then the wording in the recitals and the body of the act must at least ensure

that data processing by the public order administration is not included. Data processing by other public authorities must remain within the scope of the Regulation as provided for in the current regulatory framework.

The conference is opposed to the Council version's additional restriction of the General Data Protection Regulation in favour of the Directive in Article 2(2)(e) of the Regulation. The Regulation should apply to data processing by the public order administration and for the purpose of threat prevention.

2. Personal data must be clearly defined!

Like existing law, the General Data Protection Regulation is based on the concept of personal data. This is the logical consequence of the fundamental law and primary law guarantee in Article 8(1) of the EU Charter of Fundamental Rights and Article 16(1) TFEU giving everyone the right to the protection of personal data concerning him or her. The definition of personal data in Article 4(1) of the Regulation is therefore extremely important, because it determines whether data protection law applies.

It should be noted that a natural person should also be regarded as identifiable if he or she can be distinguished from other persons within a group and therefore treated differently from those persons. Identifiability must therefore also include whether a person can be singled out of a group, as in the Parliament's proposed text for recital 23.

The Commission's and Council's proposed wording for recital 24, that identification numbers, location data, online identifiers or IP addresses need not necessarily be considered personal data, also leads to an unnecessarily restrictive interpretation of personal data. The same criteria for determining whether they are personal data apply to these data as to all other information. Mentioning them specifically leads to the wrong conclusion that other criteria apply here. This would also contradict the rulings of the European Court of Justice.

The conference supports the Parliament's proposal for recital 23 clarifying that the possibility of singling out a natural person in a group is a means of identifying that person.

The conference demands that the Parliament's proposed text for recital 24 be used which makes clear that identification numbers, location data, online identifiers, IP addresses and other specific factors should in principle be considered personal data.

3. Data minimization must remain a design objective!

For data processing to interfere as little as possible with fundamental rights, it is essential that government and the private sector limit themselves to what is necessary to achieve their legal or legitimate purposes. Ubiquitous data processing and the use of Big Data technologies generate unimaginable quantities of (personal) data, leading to a situation which many find vaguely threatening, because government agencies or companies have the potential in this way to collect information from every area of an individual's life and analyse it however they like. This is precisely why the principle of data minimization, which has been anchored in German data protection law for years, is now more important than ever. In this way, incentives are created to design processing and business processes in away compatible with data protection.

Happily, the Commission and the Parliament have recognized this and have explicitly anchored the principle of data minimization as one of the basic principles of data protection in Article 5(1)(c) of the Regulation. It is thus even harder to understand why the Council deleted the principle of data minimization from its proposal – a troubling sign in favour of even more extensive processing of personal data.

The conference advocates explicitly anchoring the principle of data minimization in Article 5(1)(c) of the General Data Protection Regulation as formulated by the Commission and the Parliament.

4. The principle of purpose limitation must not be watered down!

Purpose limitation has long been a central principle of data protection law. It makes the processing of personal data transparent and predictable, thereby increasing the autonomy of data subjects. Given the invisibility and extent of data processing, data subjects must have confidence that their personal data are processed only for the purposes for which they were originally collected. Article 8(2) of the EU Charter of Fundamental Rights therefore anchored the principle of purpose limitation as a cornerstone of data protection.

The Commission's proposal for the Regulation largely follows the approach taken by Directive 95/46/EC: Article 5(1)(b) states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".

The current Directive 95/46/EC allows the processing of personal data for other purposes only when these purposes are compatible with the original purpose; it does not allow any other changes of purpose. As a rule, this has made it possible to balance strong protection for the right to determine the use of one's personal information appropriately with the public interests in data processing of the government and the legitimate interests of companies.

By way of derogation from this, in its proposed Article 6(4) of the Regulation, the Commission additionally provides the possibility that personal data may be processed where the purpose of further processing is not compatible with the one for which the personal data have been collected. And the Council further expands this exception by allowing such incompatible further processing when it is in the legitimate interests of the controller if these interests override the interests of the data subject. These revisions would allow changes of purpose to such an extent that the principle of purpose limitation elementary to data protection would be sacrificed, limiting transparency and the individual's freedom to decide to a problematic degree.

The European Parliament therefore returned to the proven approach taken by Directive 95/46/EC and consequently deleted Article 6(4) of the Regulation, which was also an early demand of the Article 29 Data Protection Working Party of the European data protection authorities.

A strong guarantee of purpose limitation is essential to ensure that individuals have the greatest possible transparency and freedom to decide. The conference therefore vehemently opposes the Council's proposal to water down the purpose limitation principle and advocates, on the basis of the Council's proposal, deleting Article 6(4) of the Regulation.

5. With regard to data protection law, no free pass for archives or statistical, scientific or historical purposes!

The processing of personal data for archiving purposes in the public interest, for statistical, historical or scientific purposes is subject in some cases to special rules, depending on the nature of the intended use of the data. In every case, the aim is to find a proper balance between the fundamental rights to data protection and privacy and important, in some cases also constitutionally protected interests such as the freedom of research or the public interest in official statistics or the long-term availability of government information in archives. This is recognized by the data protection commissioners of the Federation and the federal states. Up to now, the current data protection law has maintained a proper balance.

In its proposal, the Council goes in various ways beyond this approach and unacceptably privileges the areas mentioned. On the one hand, Article 5(1)(b) of the Regulation would generally always allow further processing for the purposes mentioned, thereby suspending purpose limitation. On the other hand, Article 6(2) of the Regulation would enable (further) processing for the purposes mentioned without needing the legal basis of Article 6(1) of the Regulation. This would mean that processing for the purposes mentioned without a further legal basis, subject to special national provisions in certain areas pursuant to Article 83 of the Regulation, would be possible, and the further processing of personal data originally collected for other purposes would be possible with almost no restrictions.

In addition, this privilege covers too broad a range. Only with regard to the archives in the public interest, there are no concerns, especially since at least the government archives pursuant to Article 83 of the Regulation must follow usually differentiated national law. However, in privileging statistical purposes, the Council proposal does not distinguish between official statistics and other statistical purposes. While privileging the former is understandable in the framework of Article 83 of the Regulation, there is otherwise a risk that operators of social networks, search engines, analytical tools, etc. for example could declare that their extensive profiling constitutes statistical purposes. Similar concerns apply to the privileging of scientific data processing, which the Council does not limit to purposes of scientific research.

Data protection principles apply also to the processing of personal data for purposes of public archives and for statistical, scientific and historical purposes. The conference expects the trilogue to produce a differentiated and balanced rule to protect the interests mentioned which limits the restrictions of the fundamental rights to data protection and privacy to the absolute minimum necessary. All processing for the purposes mentioned requires a legal basis in the meaning of Article 6(1) of the Regulation. Article 6(2) of the Regulation is thus misleading and should therefore be deleted. Furthermore, like archives, only official statistics should be privileged. Profiling in social networks, search engines, with the use of analytical tools, etc. must not be privileged.

6. Consent must ensure the data sovereignty of the individual!

The right of informational self-determination has always meant that the individual in principle has the right to decide whether to disclose his or her personal data and how those data are used. As a direct consequence, individuals principally have the autonomy to determine whether to allow processing of their personal data or not. Consent is crucial to effectively

ensure this autonomy. Consent is therefore explicitly mentioned in Article 8(2) of the EU Charter of Fundamental Rights as the legitimate basis for the processing of personal data.

Aware of this significance, the Commission and the Parliament decided that consent should take effect only if it is explicitly given. Only an explicit statement of consent can ultimately serve as evidence that an individual is aware of the implications of his or her decision.

In contrast to the EU Charter of Fundamental Rights, the Council's proposal departs from this principle by making unambiguous consent sufficient. This would allow globally active service providers in particular to claim broad data processing powers without the explicit consent of data subjects by using blanket data protection provisions and default settings that are not conducive to data protection. Only opt-in can be accepted as consent compatible with data protection.

Further, the operative part of the Regulation should contain a prohibition against making the use of a service conditional on the data subject's agreement that his/her personal data may be processed despite this is not necessary for the performance of the service. While the Commission and Parliament include such a prohibition in Article 7(4) of the Regulation, the Council has deleted it, only mentioning it in the recitals (recital 34).

To effectively ensure the right to determine the use of one's own data, the conference supports the approach of the Commission and the Parliament that only consent that is explicitly given can serve as the legitimate basis for the processing of personal data. Article 7 of the Regulation should also explicitly prohibit making the use of a service conditional on data subjects' agreement that their personal data may be processed for other purposes as the performance of the service.

7. Rights of data subjects

a. Ensuring that information and actions are free of charge

The Commission's and the Parliaments proposals for Article 12(4) of the Regulation state that information and the *actions taken on requests* for the exercise of the rights of data subjects are to be free of charge. By contrast, the Council's proposal says that only information provided under Articles 14 and 14a and any *communication* under Articles 16 to 19 and 32 are to be provided free of charge. This leaves unclear whether the exercise of the rights of data subjects must be free of charge or whether controllers may charge a fee. The fact that

only the right of access (Article 15) explicitly states to be free of charge (see Article 15(1) and (1b)), while the other rights of data subjects do not, speaks for the latter.

Data subjects' ability to exercise their rights free of charge is essential to ensure the effective exercise of the data protection rights. Charging for the exercise of rights typically discourages data subjects from exercising their rights.

The conference advocates an unmistakable statement to the effect that the exercise of data subjects' rights and implementation by controllers must be free of charge.

b. No restrictions on the rights of data subjects!

The right of information (Article 14, 14a of the Regulation) enables data subjects to assess the extent and risk of data processing. It is the necessary condition for creating transparency. The Council's proposal only requires providing information on the identity and the contact details of the controller, the purposes of the processing for which the personal data are intended and the legal basis for the processing. Additional information is to be required only if necessary to ensure fair and transparent processing having regard to the specific circumstances and context in which the personal data are processed.

The conference rejects restrictions on the rights of data subjects. The Council's wording leads to legal uncertainty and leaves room for interpretation resulting in a lower level of data protection than is currently in place.

In contrast to the right of access (Article 15), the information rights in Articles 14 and 14a of the Regulation refer only to general, abstract information on the type, extent and purpose of data processing. The information obligation will therefore not result in excessive bureaucratic costs, because this information can be provided to data subjects in standardized form. The conference believes the standardized information policies proposed by the Parliament with the addition of pictograms (Article 13a) are worth considering.

The conference opposes restrictions on the rights of data subjects and supports the position of the European Parliament.

c. Ensure effective limits to profiling!

The federal and state data protection commissioners believe that the proposed rules on profiling in Article 20 of the Regulation are not sufficient to effectively protect individuals

against the creation and use of personality profiles in this age of Big Data, the omnipresent Internet of Things and technologies for collecting and analysing individual data in all areas of life.

The proposals of the Commission, Parliament and Council on Article 20 of the Regulation are inadequate, because none makes profiling itself subject to special requirements, but only decisions based on automated processing (Council) or a measure (Commission) based on profiling, or measures producing legal effects concerning the data subject or similarly significantly affecting the interests of the concerned data subject (European Parliament).

The Council's proposal is especially inadequate, because, like Article 15(1) of the Data Protection Directive 95/46/EC, it reduces the phenomenon of profiling to decisions based on automated processing and having legal effects for individuals. This only covers a specific result of data processing in connection with the evaluation of personality features, but not the fundamental question of what purposes and within what boundaries personality profiles may be created and used at all. Further, in practice this approach has significant potential for interpretation and circumvention with regard to services or applications having no direct legal effects on data subjects, such as the analysis of Internet use, the analysis of personal preferences by a social network, the analysis of location data or the analysis of physical activity using apps and sensors.

In this context, the federal and state data protection commissioners call for a differentiated rule on the creation and use of profiles in the Regulation which should contain the following core elements:

- Instead of being limited to automated decision making, an approach should be chosen which covers all profiling or measures based on it. The European Parliament's proposal for Article 20 comes the closest to this approach.

- Exceptions from the prohibition on profiling need to be clearly defined. Due to their highly sensitive nature, special categories of personal data should not be allowed for use in profiles.

- In any case, the processing of personal data for profiling purposes should always be accompanied by the highest level of transparency and awareness of data subjects. Individuals must know when, for what purpose and in what form their data are processed for profiling purposes on the Internet or when using a service on a terminal device and must supply explicit consent for such processing.

- Further, data used to create and evaluate profiles should have to be anonymized or pseudonymized at the earliest possible date, the latter subject to a ban on (re-)identification.

In view of the dangers the European Court of Justice has repeatedly found that personality profiles pose to the fundamental right to data protection, the conference demands that the existing proposals on profiling should be substantially improved in line with the points outlined above.

8. Accountability for data protection applies to all processing of personal data!

Accountability for complying with data protection law, covered in Chapter IV and in particular Article 22 of the Regulation, is a central fundamental principle of modern data protection law. Controllers and processors are responsible in every case and without restriction for complying with data protection, regardless of the type, extent, circumstances or purpose of processing and of the probability and severity of risks for data subjects. Controllers and processors must also be fully able to demonstrate that they are meeting their obligations. Risk-based aspects may be considered only with regard to the question of which concrete measures should be taken to meet these obligations.

So it is necessary to make clear that a risk-based approach can only refer to *how* obligations are met, not whether they are met or the demonstration that they have been met. The Commission's proposal expresses this the most clearly by avoiding all relativizing.

The conference prefers the Commission's approach for Article 22 of the Regulation, to make clear that accountability is a cornerstone of data protection and is not open to a risk-based approach.

9. Goals relating to guaranteeing technical and organizational data protection must be anchored in the Regulation!

In order to protect fundamental rights, the processing of personal data needs not only legal, but also technical and organizational protection. To this end, modern data protection law must define goals on which the measures to be taken must be oriented. This means that in addition to the classic goals of IT security, specific goals must be added which refer to the protection of personal data. For this reason, the goals of confidentiality, integrity, availabil-

ity, non-linkability, transparency and the ability to intervene must be anchored in the Regulation. While the Commission and the Council mainly focus on the classic goals of availability, integrity and confidentiality in their proposals for Article 30(2) and Article 30(1a) of the Regulation, the Parliament's approach in Article 30(1a) and 30(2) of the Regulation in conjunction with Article 5(1)(ea) and (eb) goes the farthest.

The conference believes that Article 30 of the Regulation must clearly and consistently anchor the goals of confidentiality, integrity, availability, non-linkability, transparency and the ability to intervene. It therefore supports the Parliament's aim but would like it to be formulated more clearly.

10. Good data protection needs data protection officers in businenesses and public authorities!

Regardless of the material-legal provisions, the concrete level of data protection in businesses and government agencies greatly depends on how well data protection is accepted and what the local data protection culture is like. The data protection supervisory authorities can set the tone and make a difference with their inspections and advising. But these activities are necessarily limited in time and are not always free of conflict, due to the differing roles. This is why the institution of data protection officers in business and public administration is so important.

It is therefore good to see that, in Article 35, both the Commission and the Parliament provide for the mandatory designation of in-house data protection officers. However, the criteria chosen by the Commission and the Parliament according to which such designation is mandatory are not convincing.

Unfortunately, the Council did not agree on a Europe-wide requirement to designate data protection officers, mainly due to arguments that such a requirement would create too much bureaucracy and would be too expensive. Decades of experience in Germany refute these arguments. Without the involvement of a corporate data protection officer, compliance costs for businesses are significant, and a data protection officer can also often help avoid sanctions and fines.

The conference continues to advocate the mandatory, Europe-wide designation of data protection officers in businesses and public authorities. There should be no exceptions for public authorities; in the private sector, data protection officers should be required not only for businesses of a certain size or affecting a certain number of data subjects, but also in any

case if their data processing is associated with special risks to the rights and freedoms of data subjects.

11. Greater supervision of data transfers to government agencies and courts in third countries!

Since the revelations of Edward Snowden, there has been an intensive discussion of better protecting the personal data of European citizens against government agencies and offices in third countries. For this reason, the Parliament proposed a specific Article 43a of the Regulation which makes clear that the EU would neither recognize nor enforce decisions by courts and administrative authorities of a third country requiring controllers to hand over personal data unless required by international agreements on administrative or mutual legal assistance. In the individual case, such decisions would require approval by the bodies indicated in the agreements.

Both the conference and the Article 29 Working Party support this demand. Creating such a rule would not stop foreign intelligence services from operating in Europe, but it could create a certain amount of transparency regarding such surveillance, could help maintain proportionality and above all create incentives to conclude international agreements.

Unfortunately, the Council did not pursue the Federal Government's initiative to this effect.

The conference also advocates creating a specific legal basis for data transfers to government agencies and courts in third countries, which would create greater transparency and oversight especially in view of surveillance by intelligence agencies. The conference supports the Parliament's proposed Article 43a of the Regulation.

The competence should however be assigned as follows: If the requesting and requested states have concluded a mutual legal assistance treaty or an international agreement, the body designated in that treaty or agreement should be responsible for receiving and reviewing a request for data transfer. If the treaty or agreement does not designate a competent body, this task may be assigned to the data protection supervisory authorities.

12. Cooperation among the data protection authorities in Europe must be effective and responsive to public needs

One area in which the General Data Protection Regulation is intended to bring about significant progress is by improving cooperation among the data protection authorities in Europe. To achieve this while offering businesses added value, the Commission proposed creating a so-called one-stop shop, a consistency mechanism and a European Data Protection Board.

At the suggestion of the Council, there should be a lead data protection authority which serves as a single point of contact for a business in the place where its main establishment is located; this authority should also cooperate with other supervisory authorities concerned, whether due to additional branches of the business or because their citizens are affected. The Council also made proposals regarding the one-stop shop, so that data subjects may apply to their local supervisory authorities and courts. To arrive at binding decisions without the Commission's involvement, the Council further proposes granting the European Data Protection Board binding decision-making powers by giving it its own legal personality. The model proposed by the Council is complex for the supervisory authorities but is intended to enable citizens' concerns to be dealt with locally and to create a point of contact for businesses in case of data processing in more than one country.

The conference supports the Council's proposal on the one-stop mechanism. But the failure of the lead data protection authority to act must not be allowed to undermine the efficient enforcement of data protection law. It is necessary to create a provision allowing the member states' supervisory authorities, if their citizens are affected, to demand that the lead authority take action and to require the European Data Protection Board to immediately conduct a review if the lead authority refuses to take such action.

The one-stop shop is intended to create an appropriate balance between the various interests, to enable complaints to be processed close to where they are submitted, to give businesses a clear point of contact and to create the necessary binding nature and legal certainty by giving the European Data Protection Board a greater role. The conference asks the parties involved in the trilogue to define practical rules of procedure, especially regarding time limits and administrative assistance among the supervisory authorities.

13. In favour of strong data protection in the employment context

In Article 82, the General Data Protection Regulation leaves data protection in the employment context up to member state law. The Council and the Commission refrain from more

specific requirements, stating only that the member states must comply with the framework of the Regulation. By contrast, the European Parliament's proposed text includes very specific minimum standards.

The conference believes it is important for Article 82 of the Regulation to give the member states the possibility to require a higher standard than that of the Regulation. The conference welcomes the Parliament's approach of including concrete minimum standards for data protection in the employment context within the Regulation itself.

In the context of processing employee data, in the interest of minimum harmonization the Regulation should allow the member states to go beyond the level of data protection provided in the Regulation. The conference supports the Parliament's approach of setting concrete minimum standards.

14. The creation of the right to pseudonymous Internet use for all people in Europe!

There are many substantial reasons for using a pseudonym in telemedia services: These include the wish to avoid profiling under the real name, either to protect oneself against unlawful access, or to reinforce protection when using social networks. Moreover, a pseudonym can also provide protection against political or racial persecution or discrimination and social disadvantages, for example on grounds of sexual orientation. Pseudonyms can prevent the private use of a telemedium being misused by third parties for initiating business contacts. This is important, particularly in connection with persons subject to professional secrecy, such as medical doctors, priests, lawyers, social workers, and not least for the protection of those persons in contact with them.

The right to approach other users in telemedia principally by using a pseudonym strengthens informational self-determination and freedom of expression without excluding the possibility for the provider of telemedia to prosecute and punish abusive conduct by persons using a pseudonym. However, in the European General Data Protection Regulation, a relevant explicit rule is still lacking in the catalogue of data subjects' rights.

In order to protect the telemedia users' privacy, the Conference considers it necessary to include a provision laying down a binding stipulation for a right to pseudonymous use at least for the private use of telemedia within the EU.