GENERAL DATA PROTECTION REGULATION

CEEMET welcomes the aim of the European initiative to arrive at uniform rules on data protection throughout Europe, in order to ensure a high degree of data protection for individuals and overcome barriers to the movement of personal data. However, the overly detailed employer obligations will create more administrative burden and compliance costs for companies without a proportionate privacy benefit.

Employment relationship affected

The aim of the European initiative is to arrive at uniform rules on data protection throughout Europe, in order to ensure a high degree of data privacy and protection for every individual and overcome barriers to the movement of personal data. **This initiative is welcomed, especially since it prevents downward competition for the lowest level of protection.**

However, **we are very worried about the impact of the proposal on data processing in the employer/employee relationship.** Employment relationships are not excluded from the regulation's scope. The escape clause in Article 82 only gives national lawmakers very limited room for variation in the respective countries.

In order to be well-balanced, data protection in employment relationships should on the one hand serve the staff's legitimate interest in their personal data being protected, while on the other hand leaving companies enough leeway to implement the employment relationship.

As far as the European metal and electrical industry is concerned, the following points are essential in designing an EU data protection regulation:

- Collective agreements must be preserved as a regulatory instrument
- Consent must remain the basis for permission
- Data protection within groups of companies should be eased
- Red tape should be limited to what is necessary for an employment relationship with a special focus on SMEs
- Sanctions must be balanced

Preserve collective agreements

In several Member States, collective agreements and employees consent to the processing of their data by employers are an acknowledged basis of legal data processing. This practice should be maintained.

For day-to-day business it is necessary to create clear and unambiguous rules that are adapted to the conditions in the respective company and enable staff to work efficiently. **Collective agreements on handling data processing systems have been concluded in many EU-countries since the mid-1980's. This option must also be preserved in the future.** The number and variety of topics covered in such agreements are summarised in the annex and show that not every individual case can be regulated by the law in a legally binding way. There is a considerable need for clarification at company level.

Preserve employees' consent

Employees should have the right to make an informed choice about how their data will be processed. Therefore, the presumption that the employment relationship is of questionable nature in preamble 34 concerning consent is unacceptable. **In any case, employees must be asked for consent if personal data is to be collected and processed.** As a rule, this instrument of consent is used to grant employees additional benefits that are not directly covered by the employment relationship. In some cases,

however, it is also required to implement the employer's duty of care.

CEEMET believes that the provisions of the proposal on consent should not hinder a sensible and flexible processing of data within the employment relationship. Therefore, **we oppose the changes in the definition of consent as they will make the process too bureaucratic.**

Please find many examples for the use of consent in our companies in the annex.

Improve the exchange of information within the group

Like every international company, many of our Metal, Engineering and Technology (MET) companies operate a division-of-labour system with subsidiaries. Cooperation between staff, and therefore the exchange of employee data, is imperative in such a procedure. Therefore, we need facilitations for the processing of data within corporate groups.

Reduce delegated acts and implementing acts

The proposed data protection regulation includes 26 provisions that grant the European Commission the power to adopt delegated acts. Furthermore, 19 provisions allow the Commission to adopt implementing acts. This is contrary to article 290 of the Treaty on the functioning of the European Union (TFEU) which limits the use of delegated acts to “other than essential elements of an area”.

The use of secondary rulemaking not only undermines legal predictability for employers but also risks neutralising the effectiveness of the provisions by complicating the data protection regime. The legislation process would be constantly changing. Thus, achieving compliance for employers would be extremely difficult, even more as compliance with data protection legislation often requires significant and time-consuming data system investments.

This is especially the case for member states’ option in Article 82 to adopt national data protection rules for the employment relationship. These national laws could constantly be questioned by the Commission through the use of the delegated act in Article 82.3.

We therefore call for a limitation of delegated and implementing acts only to essential elements.

Reduce red tape to an appropriate level

The many administrative requirements of the data protection regulation are tailored more to companies whose main business purpose is to collect personal data ("lex facebook"). However, for small and medium-sized enterprises in particular the bureaucratic obligations involved in processing employee data are wholly inappropriate. A balanced level of data protection in employment relationships must, on the one hand, serve the employees' legitimate interest in the protection of their personal data and on the other hand give the company enough leeway to implement the employment relationship with a minimum of red tape.

In the annex you will find examples where the regulation could cause unnecessary burden for our companies.

Improve definition of personal data

The definition of personal data suffers from ambiguities. Personal data is defined as “any information relating to a data subject”. A person is a data subject as soon as he or she is reasonably to be expected traceable by “means reasonably likely to be used by the controller or by any other natural or legal person”. In our view, this is too broad and lacks clarity.

In order to prevent huge compliance costs and legal uncertainty a clear definition is needed. **It must also be ensured that pseudonymized data is not included within the scope of the data protection regulation if the data owner cannot de-pseudonymize the data.**

CEEMET

Council of European Employers of the Metal, Engineering and Technology-based industries

CEEMET aisbl
Bld. A. Reyers 80
B-1030 Brussels

Tel. : +32 2 706 84 65
Fax : +32 2 706 84 69

secretariat@ceemet.org
www.ceemet.org

Balance sanctions

The draft data protection regulation proposes very high administrative sanctions for violations based on a "one-size-fits-all" approach.

Example 1: Article 79.5.b. states that the supervisory authority shall impose a fine up to € 500.000 or 1% of an enterprise's worldwide turnover, to anyone who, intentionally or negligently, does not comply with the right to be forgotten or to erasure.

Example 2: Article 79.6 (h) foresees a fine of € 1.000.000 or 2% of an enterprise's worldwide turnover in case they intentionally or negligently, if do not alert or notify a personal data breach.

Even though effective and high- quality enforcement is essential, the proposed sanctions are excessive and disproportionate. Any sanction levied should be proportionate to the impact on data subjects. In our view, particularly in cases of first and non-intentional non-compliance, a warning procedure as well as pre-requisites for renouncing from inflicting sanctions should be considered.

CEEMET aisbl
Bld. A. Reyers 80
B-1030 Brussels
Tel. : +32 2 706 84 65
Fax : +32 2 706 84 69
secretariat@ceemet.org
www.ceemet.org

ANNEX: Practical Examples from Companies in the Metal and Electrical Industry

Preserve collective agreements

Examples for works agreements of a large-scale member company

A large, globally operating member company uses works agreements for a variety of purposes to ensure the necessary security under data-protection law and to actively involve the staff's representative body. This greatly increases the level of acceptance. The imputed imbalance between employer and employee when it comes to consent can be overcome in this way. Furthermore, the instrument of consent is unusable in these cases because of the large number of employees.

- Works agreement on the introduction and application of systems for processing employee-related data and information
- Works agreement on the Personal Card (a multi-functional employee ID that can also be used for paperless payments on the company premises)
- Works agreement on the use of establishment-level IT systems (see example above on the private use of email and the internet)
- Works agreement on administrators (regulates the rights and obligations of administrators: e.g. they may not pass on personal data without a legal basis even when instructed to do so by a supervisor)
- Works agreement on collecting telephone data (states, for example, that the last two digits of phone numbers may not be shown in accounting)
- Principles on the personnel data program (enables managers to access employee data that are relevant to their work area based on a strict management of user access rights). This works agreement is supplemented by numerous notes for the record governing the individual applications.
- Works agreement on employee surveys (regulating how electronic employee surveys are handled and interpreted)
- Works agreement on the electronic personnel file (regulating how long data are stored and the management of user access rights)

Preserve the employees` consent

Example 1

Business travel

The employee goes on a brief business trip to China. In this case the company has to provide the Chinese authorities with precise information on the person concerned, including data on his or her salary. For this reason, a separate declaration of consent is obtained from the employee.

Example 2

Deployment abroad

The employee is given a posting with a foreign subsidiary. Here, the company reports the employee's personal data to the foreign subsidiary (and possibly also to government authorities for visa processing).

In this case, the secondment contract expressly contains the employee's consent for his/her data to be transferred to the foreign company.

As part of the international assignment, the employee's consent is also obtained for the transfer of (tax-related) data to the appointed tax consultancy. This is necessary to enable the tax consultants to assist the employee according to contract in the preparation of his/her income tax returns both in the home country and abroad,

and ultimately to be able to carry out the agreed "tax equalisation" in the relationship between the employer and the employee.

Example 3

Corporate health management

A company takes its responsibility towards its employees very seriously and offers them healthcare and health-promoting measures (e.g. screening for colorectal and skin cancer) and immunisations (e.g. for influenza). This inevitably also involves collecting personal data on the staff, including coordination of appointments, passing on the examination findings to the employee and invoicing the service provider. This offer could not be maintained without the possibility of obtaining the employees' consent to process their data.

Example 4

Corporate integration management

A company has agreed with the works council to make effective use of corporate integration management.
According to section 84, subsection 2 of the Social Code, Book IX (in Germany) the employer is obliged to offer integration measures under certain conditions (e.g. if a staff member has health problems). Implementing these measures requires the consent of the person concerned in accordance with section 84 of the Social Code, Book IX. However, the regulation does not contain any special permission to collect and process this naturally sensitive data. It only specifies that the employee must be informed about the data processing.
The company uses a declaration of consent that has been agreed with the works council in order to create legal certainty and transparency – also for employees on what data can be processed and stored for this purpose and for how long. The data is filed separately from the personnel file – as required under German case law.

Example 5

Video analysis for the purpose of workplace design

The company attaches great importance to optimising assembly workplaces in terms of ergonomics, quality and productivity (e.g. projects on creating a work environment that does justice to the ageing process). Video analysis is used as an instrument to help make this optimisation process as efficient as possible and to ensure verifiable improvements (without disturbing employees working on the production line). Since complete anonymity of the video recording is not possible, the company seeks the consent of the employees, who can participate in the analysis on a voluntary basis. The principles for conducting the video analysis and processing the data obtained are regulated by a works agreement.

Example 6

Private use of IT systems

As in very many MET companies, the employees in this company are allowed to use its IT systems for private purposes (including private emails and private calls from company phones). The company offers its employees this possibility and has agreed fundamental rules on it in a works agreement with the works council. The company would like to be perceived as an attractive employer by its workers and avoid a competitive disadvantage in its search for skilled personnel. A ban on the private use of these systems is often seen as a deterrent these days (web 2.0 generation). To ensures that these rules are complied with, members of staff who want to take advantage of this offer must consent in advance to misuse controls.

Example 7

A company website and annual report

A company makes highly complex systems. It offers not only the product, but also extensive

customer support. This leads to a strong customer contacts in which the personal relationship between the employees and the customers is extremely important. The contact details of the staff posted on the internet therefore include their names and a personal photograph. Compliance with data protection law with regard to the publication of the photographs is ensured by obtaining the consent of the service staff. As the company operates in Germany, German law requires the employee's consent when a photograph is published (section 22 of the German Law on the Protection of Copyright in Works of Art and Photographs [KUG]).

The same applies to annual reports.

Example 8

Staff photographs on the intranet

A quite large member company regards cooperation between the individual departments as very important in many situations; it is usually achieved by telephone and via the internet, partly because there are several different locations. The company has reached a size which makes it impossible for every employee to know all the others. Office parties are no long sufficient for this purpose. Experience has shown that a photograph of a colleague at another location makes cooperation easier and that coincidental meetings can be used for personal contact. These would not take place at all without the photographs. The employees give their consent to their photographs being published on the intranet.

Example 9

Birthday lists on the intranet

The company is very committed when it comes to employee satisfaction. A staff survey revealed that there was considerable interest in being able to congratulate colleagues on their birthday and that the employees really appreciated receiving birthday wishes from colleagues and superiors. A birthday list has therefore been posted on the intranet. Employees have given their consent for this.

Example 10

Easier travel bookings by the assistance functions

The assistants in this company take care of making the travel arrangements for the staff. In order to speed up the handling of travel bookings, the assistance functions have access to the staff's private addresses, as well as their "miles cards" and rail network cards – in some cases even their driving-licence and ID data. In this way, for example, the assistants can rent a car near a staff member's home or plan a rail connection from staff member's home at the right time. The travelling employees have given their consent to this procedure.

Example 11

Staff development programme

The company is part of a corporate group. The group's philosophy calls for a group-wide staff-development system to enable it to offer employees interesting and attractive career-development opportunities, thus generating an advantage in the competition for talent. Data such as qualifications and marital status are collected and stored as part of the staff-development programme. The declaration of consent lets the employees decide what data they want to reveal and how great their interest in staff development is (e.g. only nationally or also internationally). This also makes it possible to offer family-compatible working and personnel-development models.

Example 12

Suitability examination – head for heights

A company works in the field of wind energy. The engineers employed there check, maintain and repair the installed wind turbines. The hubs on

these wind turbines (where the rotor blades are attached) are often 100 metres above the ground. To ensure their own the safety, employees must not be afraid of heights. A corresponding examination is conducted by competent doctors.

After the examination the employer needs to be informed of the outcome. This requires the consent of the employee, allowing the doctor to disclose the examination results to the employer.

Improving the exchange of information within the group

Data transfer in a large-scale member company

To be able to efficiently make the most of the advantages of an international group, this company uses data group-wide in the following areas:

- Compiling an international staff directory containing the contact data and responsibilities of all the staff members.
- Centralising support functions (IT, personnel development, reporting).
- In transnational matrix management structures (if there is a divergence between functional and disciplinary management).

In transnational cooperation on joint development processes, personal data are also exchanged via the individual work-scopes.

Reduce red tape to an appropriate level

Example 1

Compulsory electronic personnel file

In a small company with 56 employees (more than 70% of member companies have up to 99 employees), the wife of the firm's owner has up to now administered the paper personnel files. Now, however, the duty rosters, holidays and the number of sick days have to be recorded electronically.

An external service provider does the payroll accounting. Since the company is located in a rural environment, the relationship with employees is very personal.

The disclosure and information requirements regulated in articles 11 to 15 of the draft regulation de facto requires this company, too, to keep an electronic personnel file. This is because – under Article 12, paragraph 1, last sentence – steps must be taken to ensure that the person concerned can also apply for the information electronically, if data are processed automatically. Article 2 states that this regulation also applies to partially automated processing.

It would seem very strange to the employees to make an electronic application. Since the electronic personnel file involves a wide range of legal requirements and legal pitfalls, it would be unwanted and inappropriate in this company.

Such a small company would have to purchase specially written computer programs from outside vendors. Only the providers of such programs can predict what costs the individual company will face. It might also be necessary to expand the storage capacity.

The same applies to the right to be forgotten and to erasure.

Example 2

Merging of personal data as a result of the right to information

A large company with employees both in EU and abroad uses an IT-based HR management program. To prevent profiling, strict attention is paid to ensuring that certain employee data are stored separately from each other and cannot be linked (such as results of staff assessment meetings and absence rates; marital status and occupational accidents; health prophylaxis and

CEEMET aisbl
Bld. A. Reyers 80
B-1030 Brussels
Tel. : +32 2 706 84 65
Fax : +32 2 706 84 69
secretariat@ceemet.org
www.ceemet.org

geo-data from external deployments or voluntary participation in further training courses).

The right to information in Article 15 forces the company to merge this data to provide the information. This requires the corresponding electronic equipment, which would have to be specially obtained for the purpose, counteracting the regulation's principles – on data minimisation and the restriction of profiling. Just to provide this information, employers have to create a comprehensive profile of the employee which they themselves do not need; indeed, they are not even entitled to do so in their capacity as employers. In addition to this, they must also store these profiles for long periods in order, in case of doubt, to be able to prove that they have provided the person concerned with the necessary information.