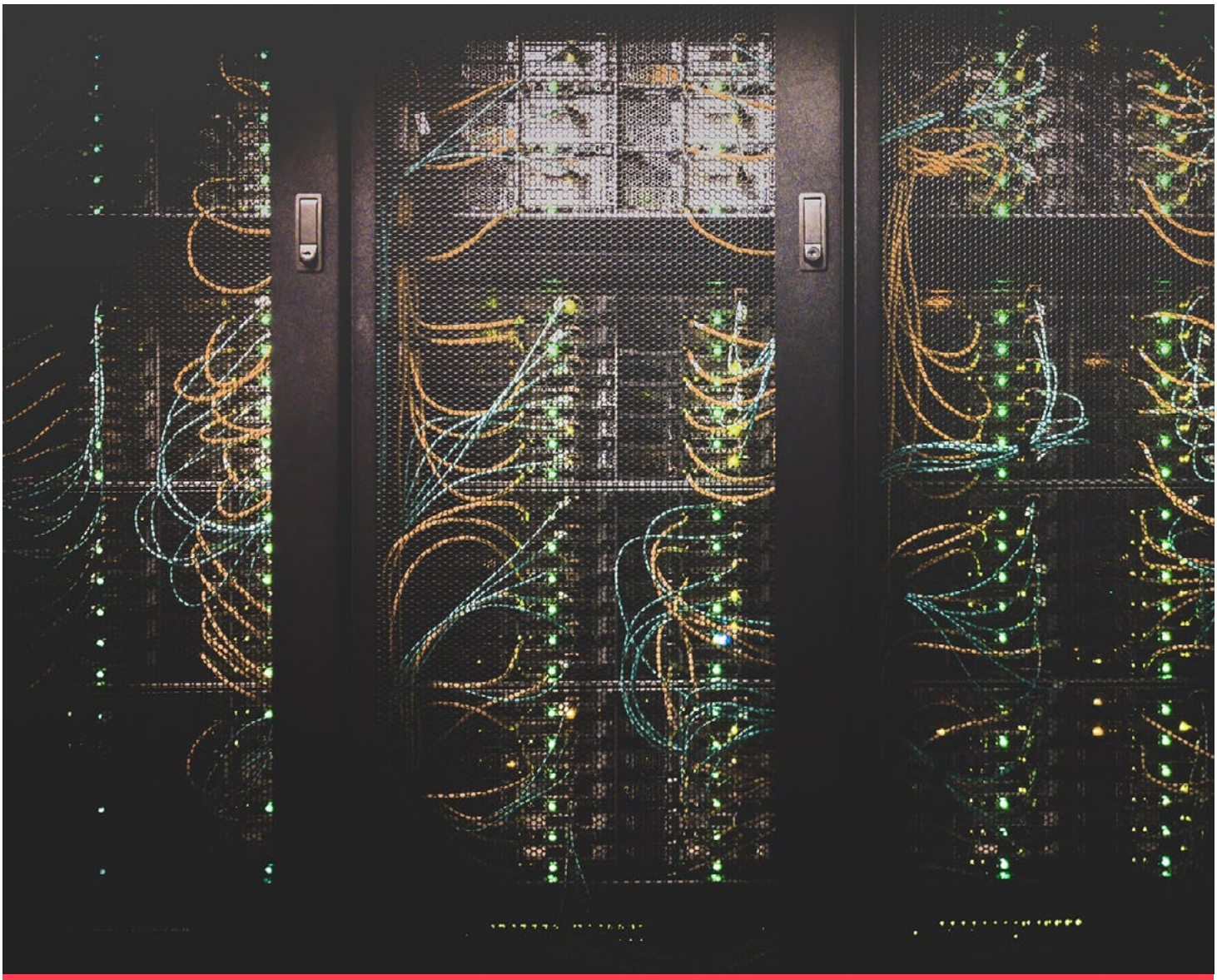
AK EUROPA

Position Paper
June 2020
EU General



A European data strategy

The AK's position

On 20.02.2020 the European Commission presented the future European Data Strategy and opened a consultation which AK would like to participate in and, in addition to answering the questionnaire, present the basic considerations outlined below.

The objective of the European Data Strategy is to create a single European data space and to ensure the security of all data. This strategy aims to ensure that citizens are at the heart of the data-driven economy, that European businesses and public authorities can make profitable use of the data they generate and that they have better access to data generated by others.

In principle, AK welcomes the project of a common European data strategy, but points out that numerous considerations regarding comprehensive data protection, balanced opportunities for consumers and data users as well as opportunities of fair competition for small companies and improved regulation of large "data collectors" must still be incorporated into the strategy. As the representative of the interests of all employees in Austria, we also pay particular attention to the effects of collecting and processing data on employees.

1. Comprehensive protection for consumers in a data-based economy

1.1. Summary of our concerns:

The aim of a legal framework "**Governance of common European data spaces**" is to clarify which data can be used in which situations for new innovative services, while respecting data protection. In this context, the Chamber of Labour is calling for:

- **Anonymisation**: A legal definition of when data can be considered sufficiently anonymous.
- **Rights of self-determination**: A clarification that, on the basis of transparent information about the intended use, consent must be obtained from the persons concerned without exception for the further use of their (initially or persistent personal) data for commercial or scientific and research purposes. Mere rights of appeal are only conceivable for applications for which the data protection authority has established an important public interest and data protection compliance in the course of a preliminary check. The opening clause in Art. 89 of the General Data Protection Regulation (GDPR) for exceptions in favour of science or statistics must be limited so that the persons concerned must be able to invoke all the rights of data subjects under Art. 12 et seqq. GDPR. Sensitive data may not be used for such data pools without the explicit consent of the data subject.
- "**Data altruism**": The "data donations" envisaged by the Commission require "donor information and contracts" to be checked in advance by data protection authorities, so that they are aware of the scope of their decision and are not merely referred to later complaints and claims for damages.

A "**legal act on data**" is intended to "clarify rights of use of jointly generated IoT data (Internet of Things, note) and rules for the responsible use of data (e.g. legal liability)". In this context, the Chamber of Labour is calling for the following **accompanying rules to protect consumers using IoT devices**:

- The owners of smart devices can have complete autonomy over the purchased product;
- They have the right of disposal over all software components and an unlimited right of self-determination over all data generated by the product;
- They can decide freely whether and who they allow to access data;
- They are free to choose repair and service companies, which also means that they can

provide the selected company with access to the required data;

- They must not be forced to accept tie-in contracts (additional maintenance and service contracts, third-party services and/or insurance offers that include tracking of product use);
- They must be able to rely on manufacturers or sellers not invoking exclusions of liability and warranty if they can choose their service companies freely or do not make all data created available.
- They must be able to use the basic functions of all smart devices offline;
- They must be able to rely on high cybersecurity standards, and compliance checked by the relevant authorities.
- They must be protected from liability allocation problems through joint and several liability of device manufacturers, software suppliers, service providers and vendors.

Under the title "**Responsibilities**" it is announced that "individuals will be assisted in enforcing their rights in relation to the use of the data they generate". New tools should enable them to decide what happens to their data ("personal data rooms") and to exercise control over their data. The Chamber of Labour has certain concerns in this regard:

- **Questionable added value**: Citizens and consumers face significant challenges in their everyday (digital) lives. For many people, having data management tasks entrusted to them represents an additional burden in terms of time and information. Privacy by Design and Default (for example, selection options via data protection settings) and data portability have been anchored in the GDPR and must be implemented in all services. New tools can therefore only refer to the very narrow field of non-personal data.
- **Data intermediaries**: Reliability, competence and independence of data trustees would have to be checked by the authorities; otherwise new risks of data misuse could arise at this level. Consumers have little need to have their data managed by a third party so long as the third party does not guarantee that the data will be used in accordance with data protection regulations and, if necessary, will enforce this. However, data protection authorities and consumer protection associations must fulfil this market watchdog role in the first place.

1.2. Of the reason for our concerns:

1.2.1 Regarding personal data

Promoting a data-driven economy requires more consumer or data protection: Politics, business and research are currently preparing the way for the transition to a data-driven economy (see inter alia the White Paper on Artificial Intelligence COM (2020) 65 or the Communications COM (2020) 66 on a European Data Economy, or COM (2018) 283 On the road to automated mobility in addition to the announcement on the European strategy for data COM (2020) 66.) Extract from the current COM communication: "Data-driven innovation will bring enormous benefits for citizens" (personalised medicine, new mobility, contribution to the Green Deal.)

Concerns of the Chamber of Labour: The drawbacks of this development should be given more room in the debate. Rights of self-determination over data, data security, freedom from surveillance constraints, discrimination against "offliners" and people who do not want to participate in every digitization trend, and those who are discriminated against by algorithmic decisions, for example, deserve equal attention.

Personal reference or not? In the above-mentioned communications, data with and without personal references are addressed as well as data where the personal reference has been more or less reliably removed. Clean separation is rare. An assessment of the Commission's projects requires clarity as to the data category in question. Much to the disadvantage of consumers, there is no clear legal boundary between the different categories of data. And with regard to (allegedly) anonymised data, experts claim that, through advances in machine learning, almost every anonymization can be traced back to an individual: consumers become re-identifiable.

Concerns of the Chamber of Labour: There is currently no legal answer as to when a personal reference still exists and when data are technically and organisationally irreversibly anonymised. There is an urgent need for action here.

Consumer confidence: The Chamber of Labour shares the Commission's view that consumers only trust "data-driven innovations" if data protection standards are complied with every time personal data are passed on. The GDPR does not (yet) meet consumer needs: Consumers do not have real self-determination over their data at the moment. The wish of two thirds of the respondents in a Eurobarometer survey is ignored in practice: they indicated that they would like to be asked for their consent before any use is made of their data.

Concerns of the Chamber of Labour: Additional efforts are needed if the self-determination rights of consumers are to be significantly improved in a data economy that demands more and more data for more and more purposes. A data-driven economy will only be trusted if weaknesses in the GDPR are improved, data security standards are regulated in a binding manner and blatant enforcement deficits are minimised.

"**Making more data available**" is the motto. The measures presented are intended to increase the supply of and demand for data. "There are currently not enough data available for innovative re-use of data, including for the development of artificial intelligence. The existing problems can be grouped according to who is the data owner and who is the data user, but this also depends on the type of data (personal data, non-personal data or mixed data sets containing both)'. The European way is "to channel the exchange and wide use of data while maintaining high standards of data protection, security and ethics". "In a society where each individual is producing ever increasing amounts of data [...] the way in which data are collected and used must first and foremost be in the interests of the individual – fully in line with European values, fundamental rights and regulations".

Concerns of the Chamber of Labour: A lack of data is not a "problem", but part of the solution: according to the GDPR, data may only be collected for specific purposes in accordance with the principles of purpose limitation and data minimisation. The statement that people are generating more and more data must also be countered by the fact that no consumer deliberately and knowingly generates large amounts of data on their own initiative. Rather, it is the providers of electronic services, the online advertising industry, etc. whose data collection and business models are a glaring contradiction to imperatives subject to penalties such as data minimisation, earmarking and privacy by design and default.

Contradiction between data economy and imperatives such as data minimisation unresolved: The prospect of a data economy combined with fundamental rights is offered, a prospect is often not feasible in actual fact. What is needed is an honest admission that sometimes there is only the option of "either...or": evaluation of large data pools for undefined purposes or a high level of data protection. The trend towards the "data wealth" of a data economy is countered by the aforementioned principle of data minimisation in the case of personal data. Anonymised data are also based on data initially collected on a personal basis, to which the admissibility and minimisation requirements of the GDPR apply. Large amounts of personal data are collected illegally without this being necessary and without a suitable legal basis, only to be used subsequently in encrypted form for commercial or scientific purposes. The need of artificial intelligence in particular for more and more training data often contradicts not only the dictates of data minimisation, but also of earmarking and privacy by design or default.

Concerns of the Chamber of Labour: Privacy and data protection must be given priority in the event of an insoluble conflict with freedom of acquisition. The obligation to minimise data must be made more concrete. It must be made clear that the requirement cannot be circumvented by collecting and temporarily storing personal data in a legally unregulated manner, only to use the data pseudonymised or anonymised for other purposes.

Consumers complain that

- Data controllers rarely obtain their consent, justifying themselves on the grounds that there is an unverifiable, overriding legitimate interest of the company or third parties in the processing of their data.

- Their data are not physically deleted, only anonymised. It is uncertain whether and how reliably anonymization is carried out. In the absence of standards and evidence, there is uncertainty as to whether it is really impossible to trace data back to them. It also annoys consumers when statistical analyses are made and sold based on their behavioural data.

- They are denied insight into algorithmic decision-making processes on the grounds that the decision is not "exclusively" but "only" partially automated, or the assessment is not associated with legal or "significantly" detrimental consequences for the consumer.

- Data is stored for years without consumers being able to assess its appropriateness. How long data are actually "required" is scarcely verifiable.

- The exact recipients of their data are scarcely ever known, only "recipient groups", because companies infer a right to choose from the GDPR and hardly ever give information about the origin of the data, since companies only have to provide "available" information, which is therefore practically never available.

- They often do not agree with their date being passed on (e.g. location data) for scientific

or statistical purposes in a form that is pseudonymised or anonymised for the user. They are annoyed if they are only given the right of withdrawal or if they are confronted with overriding predominant legitimate interests.

Concerns of the Chamber of Labour: Mandatory prior checking by data protection authorities for applications subject to an impact assessment under the GDPR. Consumers expect preventive protection. They want prevention instead of mere claims for damages in cases of violation of rights. In order to comply with the Commission's proposal following a prior check on the "fairness" of risky algorithms (see the Communication on artificial intelligence), ex ante regulatory testing will in any case be necessary in the future. This will mean that violations of fundamental rights can be prevented even before they cause major damage.

Moreover:

- Priority for rights of consent: the legal basis of "legitimate interests" should only be used in exceptional cases, which are clearly defined in law,
- Obligation to record and provide information on all specific data sources and recipients,
- Information and disclosure rights for each algorithmic decision (even if partially automated and independent of "significant adverse effects" on consumers),
- Right of data subjects to choose between physical deletion or anonymisation,
- Guidelines for the maximum data retention period in standard situations and for the implementation of privacy by design and default,
- Clarification of the controversial prohibition of the practice of tying consent to data use and access to services,
- Full extent of the rights of the parties concerned, even if the opening clause is used in favour of national rules on science and research,
- No further use of data for other "compatible" purposes without proof of a separate legal basis,
- Rights of the persons concerned even in the case of statistical attributions,
- Equipping data protection authorities sufficiently to carry out a wide range of supervisory tasks in a rapid, thorough, technically proficient and investigative manner; and
- faster procedures – because there is a lack of landmark decisions on legal issues of key cross-border importance. Without the above, the standards of the GDPR which require interpretation cannot be applied with legal certainty.

Sector-specific legislation: Sector-specific legal acts undermine the provisions of the GDPR. We see this danger all too clearly in the ePrivacy Regulation. Based on the current state of negotiations, it is to be feared that the future level of protection will be shamefully low compared to the current ePrivacy Directive. Another example: According to the EU regulation on vehicle safety, more than 20 electronic assistance systems must be installed in cars in the future. One of these is an accident data storage system that can prove to be a "data monger" for insurance companies, police, authorities and research.

Concerns of the Chamber of Labour: The level of protection afforded by the GDPR must not be undermined by the fact that data may be used extensively in sector-specific legal acts.

Data portability and data intermediaries: Consideration is being given to breaking the concentrated market power of Internet groups by granting more data portability rights to consumers or data access to competitors. This could result in yet more companies having access to user data.

European companies could emulate the excessive data processing practices of the large Internet groups. The idea of data trustees is also unlikely to satisfy the wishes of consumers: they must first be able to trust their reliability, competence and independence, otherwise new risks of data misuse may arise at this level. Consumers have little need to have their data administered by a third party, as long as the third party does not also guarantee that the data is compliant with data protection and, if necessary, enforces this.

Concerns of the Chamber of Labour: The role of market monitor is primarily played by data protection authorities and consumer protection associations, which need more resources for their various tasks.

1.2.2 Non-personal data

These data should – the rule goes – be accessible to everyone: "With the increasing amount of non-personal industrial and public data in Europe, a potential source of growth and innovation is emerging that should definitely be exploited".

Device and usage data through the Internet of Things: Items integrated into the Internet allow companies to take an even deeper look into our lives, including the creation of personality profiles or predictions about future behaviour. This development raises numerous (despite the GDPR) unresolved questions regarding privacy: When do the operating data of networked devices have a personal reference and who do they actually belong to? Consumers run the risk that their right to self-determination over their data or their rights of ownership over purchased smart products is not adequately respected. For example, a AK study (https://www.arbeiterkammer.at/infopool/wien/Privatsphaere_in_Online-Spielen.pdf) revealed that popular digital games only work with an online connection, even if played by only one person. Without a corresponding prohibition norm, users of smart devices will in the future often be forced to watch their data being tapped relatively powerlessly. All in all, a blatant informational and contractual imbalance in the legal positions between the providers involved on the Internet of Things and their customers is becoming apparent.

Providers use contractual and technical design opportunities to analyse and commercially exploit personal customer data and operating data from devices; they take little responsibility for immanent risks (software errors, cybersecurity attacks, data breaches, insolvencies of other providers also involved, damaging use of poorly developed algorithms and artificial intelligence) and rarely invest sufficiently in preventive security.

Concerns of the Chamber of Labour: Without strong intervention via consumer policy, many of the open questions on data protection, data security but also fair contracts are likely to be answered, without due regard for consumers, and in the interest of manufacturers. Incorrect results and conclusions from evaluations of device data based on the use of algorithms and artificial intelligence will also have negative impacts on consumers. There is no adequate protection against discrimination in sight.

GDPR opening clause for science, research, statistics: Art 89 opens up too much scope to undermine the rights of the persons concerned, to the detriment of consumers. What a scientific institution is actually not determined. This means that even Internet giants that conduct market research, for example, could rely on national privileges benefiting science and research. There is no clear boundary for commercial activities.

Concerns of the Chamber of Labour: In order to keep exemption in the GDPR for the purposes of science and research within reasonable limits, the regulation must define who the privileged institutions are. If data subjects' rights are to be affected, data protection authorities must carry out prior checks. In the course of this procedure, it must be certified that the objective of the research is of important public interest.

2. Market-specific regulation of digital infrastructure facilities

With regard to the creation of clear and fair rules for data access, market-specific regulation should also be considered, especially for the large platforms; this would make it possible to define ex ante mechanisms that guarantee non-discriminatory access to data, insofar as data protection regulations permit. As stated in the EU Commission's document, this has already happened in those areas where market failures have been identified, e.g. in the automotive industry and payment services.

It has long been known that large online platforms tend to be monopolies or oligopolies due to their characteristics. Because of the interaction of various mechanisms such as network effects, economies of scale and lock-ins, large Internet platforms have the characteristics of classic infrastructures. While classic infrastructures, such as the electricity grid or rail networks, are publicly regulated, large online platforms set their own rules and act as private rule-setters and "gatekeepers". Numerous cases taken up by the competition authorities also point to market failures in this area. It is not to be expected that major Internet platforms such as Amazon, Google, Facebook, Uber, booking.com and Airbnb will lose their dominant market positions in the foreseeable future.

The major Internet platforms therefore not only have the essential technical infrastructure ("essential facilities") for digital services (online trade, online advertising, various booking portals, search engines, social networks), but also possess a large pool of data relevant to competition. This large quantity of data is a prerequisite for the further development of digital business models and can also transfer an already strong market position for these companies to

neighbouring markets.

In the opinion of the Chamber of Labour, ex-ante regulation is also required for these "large data collectors", as the EU Commission has already indicated.

Ex ante, market-specific regulation, which should initially be applied at least to large Internet platforms or digital companies with marketpower, can stipulate essential tasks such as data access, interoperability, data transparency and transparency of algorithms prior to a solution.

However, provision should also be made for out-of-court settlement of disputes and, ultimately, consideration should also be given to restricting excessive use of data and data links if a massive imbalance were to arise between the provision of data and the resulting data benefit.

3. Preventing concentration trends in cloud services as well

With regard to the growing importance of cloud services, the undesirable developments familiar from the growth of platform services should also be avoided from the outset in this area. It is essential to prevent concentration tendencies and to promote and allow competition. In addition, high priority must be given to the aspect of security. In particular, it is also necessary to strengthen the independence of the European data economy as a critical and sensitive infrastructure vis-à-vis service providers in third countries and to retain a certain autonomy.

4. Competitive access to data

Companies or organisations are also being asked in the consultation procedure whether they have encountered difficulties in using data from other companies and what specific difficulties they have encountered. Both the refusal of data access and unaffordable prices were listed.

In the opinion of the Chamber of Labour, the evaluation of this question should also be used as an opportunity to initiate competition investigations if there are difficulties in accessing data.

5. Data management and workers' rights

IT systems are becoming increasingly diverse and complex. The amount of employee data generated and used is growing exponentially, and the technical possibilities for linking and analysing this data are becoming more and more sophisticated and meaningful, even including the creation of behavioural predictions for workers (profiling) and the use of automated decision-making in the area of personnel management. The European data strategy must also pay more attention to this issue and develop protection mechanisms. Co-determination rights in particular are decisive for this: These can be rights to consent or veto for individual workers with regard to data processing, but above all – in light of the position of inferiority of individual workers in negotiations vis-à-vis the employer – rights to information, effective involvement, consent or veto for employee representatives of individual companies or sectors.

6. Weighing up the policy objectives envisaged

Ultimately, the EU Commission must also weigh the policy goals it is pursuing against each other. Promoting driverless cars, for example, could lead to more private transport if the appropriate accompanying measures are not included, thus contradicting the objective of climate protection.

Likewise, the increased use of data streams and cloud services is expected to lead to increasing numbers of highly energy and resource-intensive data centres and server farms. For this reason, the risks and possible effects on the environment must also be addressed further and in more detail.

7. Broad involvement in the discussion process

In principle, there are winners and losers in every technological development – also in a data economy that is gaining in importance. In the opinion of the Chamber of Labour, mitigating measures must therefore also be seriously discussed in this area. The widest possible involvement of social partners and the relevant actors from civil society is urgently needed and must be identified and implemented in the Commission's projects.

Contact us!

In Vienna:

Daniela Zimmer
T +43 (0) 1 501 651 2722
daniela.zimmer@akwien.at

Ulrike Ginner
T +43 (0) 1 501 651 2142
ulrike.ginner@akwien.at

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

www.arbeiterkammer.at

In Brussels:

Alice Wagner
T +32 (0) 2 230 62 54
alice.wagner@akeuropa.eu

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

www.akeuropa.eu

About us

The Austrian Federal Chamber of Labour (AK) is by law representing the interests of about 3.8 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 Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.

The main objectivs of the 1991 established AK EUROPA Office in Brussels are the representation of AK vis-à-vis the European Institutions and interest groups, the monitoring of EU policies and to transfer relevant Inforamtion from Brussels to Austria, as well as to lobby the in Austria developed expertise and positions of the Austrian Federal Chamber of Labour in Brussels.