AK EUROPA

Position Paper
August 2022
Consumers

COM(2022) 197

Regulation on the European Health Data Space

Analysing sensitive health data is also possible without compromising data protection rights!

Executive Summary

The purpose of the draft regulation is to:

- provide "researchers, innovators, policy makers and regulators" with EU-wide access to electronic health data. Both public and private "data holders" shall be required to provide data collected for health care purposes to a health data "ac-cess body", which shall also provide this data to data users in a pseudonymised (indirectly personal) format (i.e. they could be indirectly attributed to a natural person) across the EU.
- shape "a genuine single market for digital health products and services" and
- facilitate access by natural persons to their electronic health data generated in the course of health care provision.

Key points at a glance

- Compiling health data and evaluating them scientifically can help to improve diagnosis and treatments and contribute to quicker and more effective health policy decisions. The Austrian Chamber of Labour (AK) therefore fundamentally supports efforts to make better use of health data. However, the question of who is granted access to the use of health data, as well as why and for what purpose, must be regulated transparent-ly for data subjects in compliance with data protection standards. In particular, any traceability to individuals must be ruled out unless there is express consent to the use of health data.
- The initiative is highly sensitive in terms of fundamental rights. The following position paper addresses the initiative's impact on consumers/ patients and their right to privacy. Health policy aspects are not considered.
- The protection standards of the General Data Protection Regulation (GDPR) are undercut.
- In a sweeping and indiscriminate manner, the right of self-determination of data sub-jects affected by the intended processing has been pushed aside to make way for the interests of the data economy in exploiting such data.
- Under the draft, data subjects would not be able to influence the further use of their health data and a wealth of other data (factors influencing health, such as individual behaviour, income etc.). They would have no right of consent or revocation, alt-hough their (indirectly) personal data may be used for all conceivable political, sci-entific and commercial projects in which there is an actual or purported public interest.
- Data subjects would not know who is using their data, the location of such use, which data are being used, for what purpose, and for how long. If the Commission has its way, the obligation under the GDPR for information to be provided to an indi-vidual about who is performing data analysis on their data and for what purpose would no longer apply. Only extremely general information about granted data per-mits is to be published on websites. The right under the GDPR to request detailed in-formation is only explicitly described for "primary use" of data (i.e. for the provision of health care services). In the case of "secondary use" of data (further processing for entirely different purposes), this right is already curtailed in effect by the fact that data subjects will not even learn in which data permits their data are included.
- Protection against data misuse is not regulated to any substantial degree in the draft. This is a gross lack of due diligence: centrally retrievable data sets of this size and high commercial value, along with EU-wide access, almost inevitably will also give rise to abusive, criminal practices.
- A serious evaluation of all consequences of the regulation is hindered by the fact that the Commission reserves the right, in countless places in the draft, to adopt del-egated acts for technical/ organisational implementation.

AK's Position

Demands from a data protection and consumer perspective

AK rejects general priority of data use over the confidentiality interests of the data subjects as such prioritisation is contrary to the GDPR due to its undifferentiated nature. If the public's trust in the use of their health data for research purposes, for example, is to be strengthened rather than lost, a concept is needed that respects the GDPR and, in particular, the self-determination of the data subjects concerned. Due to the extent of the encroachment upon the privacy rights of consumers/patients/citizens, the European Data Protection Supervisor and the Data Protection Board must be involved and the draft needs a fundamental revision.

The scope of the data is far too broad and vague: merging all health data with all conceivable socio-demographic behavioural data would enable the creation of a unique individual behavioural profile that would dwarf previous commercial behavioural profiles in the digital economy. The draft also includes blanket authorisation of matching with data from all other areas of life in completely unspecific "emergency situations". Under the draft, the health data that are permitted to be processed for secondary use should be "flexible enough to accommodate the evolving needs of data users", especially including data with an influence on health (see recital 39). This includes

- health care system data, such as electronic health records, data on health insurance claims, disease registries, genomic data etc.,
- as well as data with an impact on health, such as consumption of certain substances, homelessness, health insurance, minimum income, professional status and behaviour.
- data generated by individuals themselves, such as data from medical devices, wellness apps or other wearable devices and digital health applications may also be included.
- allowing data users to enrich the data with entirely different data and to provide the "improved" data sets to the original data holder free of charge.
- registry data, such as the vaccination registry and many other registries.

Who those "data holders" are who must provide their data for further processing is not specified: the scope of addressees is not defined with any degree of legal certainty. They could be "public, non-profit or private health or care providers, public, non-profit and private organisations, associations or other entities, public and private entities that carry out research with regards to the health sector".

It is possible for the data to be traced back to identifiable individuals: data subjects would have to expect that highly sensitive data, entire behavioural and health profiles, as well as correlations and analyses thereof might be specifically traced back to their person. The draft contains no guarantee of protection in this regard. Moreover, individual provisions and the recitals indicate the firm assumption that health data access bodies will allow data to be accessed in such a way that it is conceivable for the data to be traced back to individual persons.

In some cases, the information on certain natural persons (!) (e.g. genome data of natural persons with a certain disease) – as the Commission states in recital 41, for example – could support the diagnosis or treatment of other persons. Further, "any attempt to use the data for any measures detrimental to the natural person, to increase insurance premiums, to advertise products or treatments, or develop harmful products should be prohibited" (see Article 35 and recital 41). These clarifications or prohibitions on use would not be necessary if the Commission were confident of the impossibility of data being traced back to specific individuals in the course of further processing of pseudonymised data.

The right of self-determination is completely disregarded: according to Article 33(5), in cases where the consent of the data subjects is required under national law, the health data access body shall simply refer to "the obligations laid down in this Chapter" when granting access. In view of the fundamental prohibition on processing health data, standards for encroaching upon this fundamental right

must be formulated with particular precision. The draft fails to satisfy that requirement. The rights of data subjects to information under the GDPR are simply eliminated, which means that data subjects generally do not learn about the secondary use of their data and cannot defend themselves against suspected violations of the law.

Oversight by independent data protection authorities (DPAs) is effectively eliminated. New "access bodies for data use" are to enforce the regulation and authorise data access. Their supervisory aim is to ensure that data access across the EU is as unhindered as possible. Safeguarding fundamental rights is not among their purposes. The access bodies are supposed to "cooperate" with the DPA in a way that is not clearly defined. However, the DPAs' decision-making authority or at least power to participate in data authorisation is not safeguarded at all. It is important for the confidence of data subjects in initiatives with such weighty implications for fundamental rights that there is a strong and well-integrated supervisory body safeguarding their fundamental rights interests.

Data-driven research, policy control and commercial innovation generate benefits, but they must comply with fundamental rights. The interests of the data economy can and must be fulfilled in a way that affords greater protection to data subjects. Use must be limited to anonymised, synthetic data or data for which consent has been obtained from the data subjects.

Processing exemptions should only apply to carefully considered, key public health interests: in this way, consent of each individual could be required, as a rule, for particularly sensitive categories of data. If the data user demonstrates a substantial public interest in their research subject and professional competence, the data protection authority could substitute its authorisation of the project for the individual consent of the data subjects. A panel including representatives of the data protection authority, the data user and data holder, and the data subjects should carry out the balancing of public and individual interests. In the case of data and purposes that do not require a high degree of protection, it is conceivable that they may, as a general rule, be permitted to be further processed unless the data subject objects after being informed in detail about the given project.

Notable security and sanctions are lacking: such a centralised approach, which aims to exchange data from countless sensitive applications that are separate from each other, neither corresponds to the state of the art in security technology due to the ease with which it can be hacked, nor does it provide sufficient assurance that highly problematic personal profiles will not be created across a wide variety of applications. Provisions for strict liability/liability insurance must be included so that data subjects can easily obtain compensation without having to file a lawsuit if their data are stolen or used inappropriately.

General remarks on the aims of the proposal:

- **Primary use of health data:** the draft aims to improve **"continuity of healthcare" during stays abroad**. In cases where an individual travels to other Member States or changes residence across borders, easy electronic access to health data is also intended to improve care and treatment outcomes.

- **Patients should have rapid access to their data**, which is processed in the course of health services. Specifically, the existing right of access under the General Data Protection Regulation (GDPR) has been extended in terms of the time within which access is to be provided. Under the draft, everyone is to be able to access their own data "immediately, free of charge and in an easily readable, consolidated and accessible form". The processing deadline of one month under the GDPR does not apply.

- **A single market for health data is intended to facilitate provision of health services across borders.** The technical infrastructure for storing health data is neither standardised nor interoperable between Member States or within Member States. Systems developed separately would first have to be merged.

- **The key aim is to give the data economy unfettered access to raw material for the development of new products and services, as well as for research and policy making.** However, fundamental rights are tied to that raw material. Under the draft, the exploitation of data should take precedence over data subjects' confidentiality interests, though fundamental rights protect these. Any company, person or institution pursuing certain secondary use purposes should be able to access the vast data pool throughout the EU. This will require all "data holders" in the "health and care sector" to release their trove of data on a personal basis to national "health data access bodies". Under the draft, the access bodies shall provide anonymised data in the first instance. If data users are not satisfied with that (which is probably the rule, if the intention is to produce studies on developments over time), pseudonymised data are provided without further ado. These have an (indirect) personal reference, are highly sensitive (need to be protected) and

are therefore subject to the full application of the GDPR. What is incomprehensible here is that the data protection authorities play no role in approving the use of data by the "health data access bodies". Yet, in AK's opinion, this would be essential in order to safeguard fundamental rights and ensure an appropriate balance of interests.

- **A free ride for the data economy:** the chief aim of the regulation is therefore the introduction of blanket permission for the secondary use of health data. The regulation supersedes the GDPR, under which the permissibility of further processing is dependent on many considerations. Under Article 6(4) of the GDPR, data may only be used for a purpose other than the one for which they were collected if 1) the data subject has given his or her consent, 2) it is permitted by law and it is a necessary and proportionate measure in a democratic society, or 3) the further processing is compatible with the original purpose of collection – narrowly interpreted on the basis of the expectations of the data subjects.

- **With reference to overriding legitimate interests, the regulation takes precedence over the GDPR:** the concept of the regulation overrides Article 6(4) of the GDPR (strictly limited possibilities of secondary use) and Article 9 of the GDPR (prohibition on processing of health data with some strictly limited exceptions) in practically every respect.

    - Is the consent of data subjects to further processing required? No, this is not provided for.

    - Many of the further uses permitted under the regulation are not compatible with the original purpose and should never be permissible under the GDPR: data subjects will not expect such uses (and are not required to expect such uses), but will be surprised to find their (pseudonymised) data suddenly appearing everywhere (Article 6(4) a and b of the GDPR). Furthermore, the data, without exception, are particularly sensitive (Article 6(4)(c)).

- **Data-hungry AI:** the GDPR is seen as a hindrance to artificial intelligence (AI) research with respect to acquiring training data. Via mandatory data provision by all health and care professions, mass training data would be available for the first time for the development of artificial intelligence (AI). These would not be available to this extent at all if the GDPR were observed and without the blanket permission for processing under the present draft. Moreover, many AI experts say that data from "real" people are not needed. Synthetic data, i.e. artificially generated data behind which there is no real person, does not reduce the quality of results, but does protect real people from misuse of their data.

- **No safeguards against misuse:** are there safeguards in the form of maximum data security and draconian sanctions for breaches of due diligence? No, such safeguards are entirely missing from the regulation. Health data access bodies are only liable for authorised use, but not for misuse. The regulation does not set out precise requirements for the technical degree of anonymization and pseudonymisation. Re-identification of the individual is therefore not effectively excluded. The only requirement under the draft regulation is that the data user must not reidentify anyone. Technical data protection, which technically prevents data from being traced back to an individual, rather than relying on the honesty of the data user, is not provided for.

- **Data can be traced back to individuals:** the public access bodies should apparently have access to direct personal data, since they are allowed to notify specific individuals (and their treating physicians) if any data analysis (of which the data subjects concerned are not even aware) comes to a conclusion that has "implications for the health status" of the individual. To give a pointed example of the possible consequences: "As we have statistically/specifically ascertained about your person, you are likely to be a carrier of a genetic defect which, if untreated, will probably limit your life expectancy by X years." Access bodies are not subject to the confidentiality obligations of physicians and should not be assigned tasks that require a trusting patientphysician relationship.

- **Doubts about compliance with fundamental rights:** under Article 9 of the GDPR, health data may only be processed if the data subject has given explicit consent to the processing or if processing is necessary for preventive medicine, assessment of working capacity, medical diagnosis, treatment or health care management and is authorised by law. Vital or substantial public interests, protection against serious cross-border health threats or ensuring high standards of quality and safety (in the fields of health care, medicines and medical devices) may also justify the processing of data. However, specific legal bases and measures are always required "to safeguard the rights and freedoms of the data subject, in particular professional secrecy". Union law may only provide for the processing of health data if it "is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance

with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

AK doubts that these conditions will be met: In view of the scope and depth of the encroachment upon fundamental rights (curtailment of transparency rights, no rights of consent/ objection), blanket permission for secondary use of personal data curtails the essence of data protection law.

Our detailed evaluation:

Art 1 – Goals

According to paragraph 4, the GDPR remains unaffected. AK considers that statement to be incorrect. The blanket possibilities for the secondary use of personal health data go far beyond the permitted purposes under Article 9 (derogations to the ban on processing of health data) and Article 89 of the GDPR (use of data to facilitate scientific, statistical and research purposes).

Concerns of AK: The draft should be revised in consultation with the EU Data Protection Supervisor/ Data Protection Board in compliance with the GDPR.

Art 2 – Definitions

"Electronic health data" include not only data "concerning health and genetic data" but also data referring to "determinants of health". Since virtually all sociodemographic characteristics (especially housing, education, work, family and income) and all aspects of lifestyles, preferences and behaviours can influence health. This broad definition paves the way for access to virtually all data about a person. That in turn enables fine-grained personal profiles.

Concerns of AK: An exhaustive specification of data that may be collected would therefore be an important instrument to ensure data access complies with fundamental rights.

"Wellness applications" are devices or software used by consumers for purposes other than health care, such as "well-being and pursuing healthy life-styles".

Concerns of AK: Since consumers neither expect nor are required to expect that these data will be used for all conceivable purposes via a central retrieval point – and in view of the fact, moreover, that these data are often of dubious quality – there is no reason for their inclusion in the draft. The definition should be deleted without replacement.

Art 10 Digital health authority – Art 10

The digital health authority's responsibilities include implementation of Chapters II and III. In an annual activity report, it is only required to provide information on cooperation with the bodies responsible for data protection, cybersecurity and artificial intelligence.

Concerns of AK: The authority should share tasks with the data protection authority (DPA) in a legally secure manner through legal provisions.

Art 12 – MyHealth@EU

This platform, established by the Commission, intends to facilitate the exchange of data between national contact points for digital health. Under the draft, all health care providers shall be required to be linked to national contact points for eHealth and share data, and are joint controllers of the data on the MyHealth platform under data protection law. Under the draft, prescriptions accessible via the MyHealth platform must also be redeemable across borders at traditional and online pharmacies. Delegated acts of the Commission are to ensure "the security, confidentiality and protection of electronic health data". The responsibilities of all parties involved are to be defined by the Commission in delegated acts.

Concerns of AK: Security measures must be a core part of the initiative, especially since centralised data storage and EU-wide data-transfers on this scale are likely to be particularly prone to abuse and attract criminals. Against this background, special liability provisions must also be included so that data subjects can easily obtain compensation without having to file a lawsuit if their data are stolen or used inappropriately. Regarding the criticism of delegated acts, please see under Article 5.

Art 14 – Interplay with legislation governing medical devices and AI systems

Any entity that manufactures medical devices or high-risk AI (artificial intelligence) that is interoperable with electronic health records must also comply with the interoperability provisions of the regulation. Existing provisions "for the procurement, reimbursement, financing" of electronic health record systems may be retained.

Concerns of AK: High-risk AI, as the name already indicates, poses risks that are difficult to calculate and control. Accordingly, it would not be appropriate for

data analytics from high-risk AI to be readily shared via interoperable electronic health record systems across EU-wide infrastructure. The consequences of biased results and incorrect conclusions could be fatal in the health sector.

Art 33 – Minimum categories of data for secondary use

Each data holder is required to provide highly sensitive data to a significant degree: data from health records, data "impacting on health, including social, environmental behavioural determinants of health" such as insurance status, professional status, education, lifestyle, wellness and behavioural data, genetic or genomic data, data from the "Internet of Things" such as fitness trackers and wellness apps, from public agency medical registries, from clinical trials and "enrichments" with other data. Data holders required to share data include both the public and private health and care sectors, as well as entities that carry out research and EU institutions.

Paragraph 5 states: "Where the consent of the natural person is required by national law, health data access bodies shall rely on the obligations laid down in this Chapter to provide access to electronic health data." In emergencies (according to the vague definition in the draft of an EU data law, which has also been heavily criticized by AK), the health data under paragraph 6 may also be merged with completely different data.

Concerns of AK: Due to the extent of encroachment upon fundamental rights, we firmly reject this provision. The types of data and the parties obliged to hand them over are not specified in such a way that it is possible to speak of a sufficiently clearly determined intervention standard. Furthermore, the intended scope of the data is also disproportionate: all conceivable behavioural data could be required and analysed on an indirectly personal basis. The disclosure obligations under Article 33 appear to take blanket precedence over the right of consent under data protection law. This is unacceptable. The provision should be deleted without replacement, as should paragraph 6, which provides blanket authorisation for matching with other data in entirely unspecific "emergency situations".

Art 34 – Secondary uses

Further processing purposes include "activities for reasons of public interest in the area of public and occupational health", supporting public sector bodies or Union institutions, agencies and bodies, education or teaching activities, scientific research, and training of algorithms and AI systems that contribute to the public health or social security. Personalised health care is also listed here. Paragraph 3 stipulates that under the draft data law "access to privately held data for the purpose of preventing […] public emergencies shall be ensured".

Concerns of AK: the purpose descriptions are far too vague and unspecific and do not therefore constitute a suitable legal basis for encroaching upon the data protection rights and privacy of data subjects. The right of access to "private data" of any kind (what data and from whom?) in an emergency is so vague and excessive that the only possibility here is deletion without replacement.

Art 35 – Prohibited secondary use

The Commission itself does not believe that the present concept is unobjectionable in terms of fundamental rights and poses no risks. This provision cannot be interpreted otherwise. It prohibits "taking decisions detrimental to a natural person based on their electronic health data", for example by excluding consumers from insurance contracts or increasing premiums. Among other things, advertising and marketing aimed at consumers are prohibited, as is the development of products and services that may harm individuals and society.

Concerns of AK: If no conclusions could be drawn about the data subject upon further processing of their pseudonymised data, there would be no need to state that nobody shall suffer any detriment from decisions based on their data. The prohibition on further processing of data resulting in an individual being excluded from an insurance contract or having their insurance premium changed is of a similar nature. It is apparently expected that analyses may in fact – if performed in an unauthorised manner – be attributable to a particular individual and not contribute to the public good. Given the potential risks described above, it is unacceptable that data subjects are denied any self-determination concerning the use of their data.

Art 36 and 37 – Health data access bodies

The bodies act autonomously (are not subject to instructions) and "shall actively cooperate with stakeholders' representatives, including patients' representatives", i.e. with data holders and users.

Concerns of AK: Despite the immense sensitivity of the initiative in terms of fundamental rights, cooperation with the data protection authorities (DPAs) is mentioned only in passing: the health data access bodies are to cooperate with them and notify them of data misuse under Article 43. What would be needed is a preliminary review by the DPA of the privacy compliance of each project before the access

body initiates an authorisation process. The nature of collaboration with other stakeholders also remains undefined. In particular, patients' representatives are not granted any vested rights.

Art 38 – Obligations of health data access bodies towards natural persons

The access bodies are not required to provide each person with information under Article 14 of the GDPR about the use of the data subject's data. It is sufficient for general information about all issued permits to be published. In other words, the data subject does not learn whether, by whom, for what purpose and to what extent their data are used. This leaves data subjects in the dark as to whom they can address requests for information to under the GDPR and how they can check the lawfulness of the processing.
If the access body obtains a finding from a data user that, may affect the health of a particular individual, the access body may notify said individual (and the individuals treating physicians).

Concerns of AK: The rights of data subjects are being undermined in an unwarranted manner. Transparency about processing is a core element of the fundamental right to data protection. It is unacceptable that the obligations of data processors to provide information individually, as set out in the GDPR, have been dropped. Any form of legal protection requires knowledge of the processing of one's own data.

Art 43 – Penalties by access bodies

The access bodies shall monitor data holders and data users. They are to impose fines if data holders obstruct or delay data use.

Concerns of AK: It should be explicitly stated that the DPAs are subject to a pre-authorisation obligation with regard to GDPR compliance and a monitoring obligation in cases where analysis is conducted based on personal data. Penalising data holders is extremely problematic, as the reason for restricting access may also be doubts about the legal conformity of data access. Data holders (such as physicians and hospital staff) are also obliged to maintain patient confidentiality.

Art 44 – Data minimisation and purpose limitation

The access body shall provide anonymised data in the first instance. If the purpose of processing cannot be achieved with such data, the data shall be provided in pseudonymised format. Data users shall not "re-identify the pseudonymised data", and if they do so, "appropriate penalties" are to be imposed.

Concerns of AK: Since there is a preference for collecting and presenting developments regarding a person over time, anonymised data are often not sufficient. The approach that only the data user is subject to the obligation to refrain from re-identification must be firmly rejected. The data user may act in a careless manner or dishonestly from the outset. Consumers and patients must never be exposed to that risk. In AK's opinion, it is incumbent upon the access body to anonymise or pseudonymise data in such a way that re-identification is all but impossible. On this point, see the distinction between technical, factual and absolute anonymity.

Art 46 – Data permit

The access bodies shall check whether the request serves the purposes listed in the regulation, whether the data are necessary and whether the applicant meets the requirements under the regulation. Once the permit has been granted, which is valid for up to five years and can be renewed, the access body shall immediately request the data from the data holder. Data users shall publish anonymised results "including information relevant for the provision of healthcare" within no later than 18 months. They shall also inform the access body under paragraph 12 "of any clinically significant findings that may influence the health status of the natural persons whose data are included in the dataset". Under paragraph 14, the liability of the access body is "limited to the scope of the issued data permit until the completion of the processing activity".

Concerns of AK: It is essential that the DPA be involved in the authorisation process. Amongst other things, it must check whether the data subjects have given their consent/objected to under the GDPR or whether there is such an important public interest in the specific data exploitation that authorisation by the DPA may serve as a substitute for the individual consent of the data subjects. It also imposes conditions to ensure data security, for example. Paragraph 12 concerns highly personal decisions of each individual as to whom to entrust what data, including medical secrecy: without the data subject's prior consent to the project, paragraph 12 would have an unjustifiable impact on personal rights. The liability of the access body should be set out as strict liability and it is essential that it should also cover further processing for other purposes constituting misuse. In the event of misuse by the data user, the access body should likewise be required to compensate data subjects and would subsequently be able to exercise recourse against the infringing party.

Art 50 – Secure processing environment

The access bodies are to minimise risks of misuse through "state-of-the-art" technological means. Data

users shall only be able to download non-personal data from the secure processing environment.

Concerns of AK: The provisions are unclear and even contradictory. Users are only allowed to publish anonymised results. This obligation is meaningless if they can only download "non-personal" data in any case. Under Article 44, data users are not allowed to recreate the identity behind the pseudonymised data. That possibility would also have to be ruled out if only completely anonymised data can be downloaded anyway.

Contact Us!

In Vienna:

Daniela Zimmer
daniela.zimmer@akwien.at

In Brussels:

Alice Wagner
alice.wagner@akeuropa.eu

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

www.arbeiterkammer.at

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) represents by law the interests of about 3.8 million employees and consumers in Austria. It acts on behalf 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 objectives of the AK EUROPA Office established in 1991 in Brussels are the representation of AK towards the European Institutions and interest groups. Other objectives are the monitoring of EU policies and transfering relevant iInformation from Brussels to Austria, as well as to lobbying the expertise developed in Austria and positions of the Austrian Federal Chamber of Labour in Brussels.