AK EUROPA

Position Paper
February 2021
Digital

Data Governance Act – High data volumes require more data protection

COM (2020) 767

Executive summary

The Chamber of Labour sees this as an extremely sensitive project in terms of fundamental rights: Directive (EU) 2019/1024 on open data and the reuse of public sector information already contains a legal framework for the innovative, commercial utilisation of public sector data. However, this legal act also contains an important restriction in that the rights of third parties may not conflict with the reuse of data. This draft will allow the data economy to access protected data, although compliance with a few requirements is stipulated. In other words, data that must be kept under lock and key or can only be used with the consent of the legal owner for reasons of data protection, intellectual property rights, or business secrets can - but do not necessarily have to - be provided by public sector bodies. The fact that such a proposal is extremely sensitive in terms of fundamental rights requires no further explanation. Thus, in the opinion of Chamber of Labour the accompanying protective measures must be selected with special care. While the promotion of innovative data management is very clearly formulated, the accompanying provisions that protect the rights of data subjects are unjustifiably vague.

A positive assessment of this proposal will depend on whether the rights of third parties can still be protected reliably when opening up access to protected data. In our estimation this is unlikely to be the case. Consumers, patients, citizens, etc. will not be able to trust data transfer readily because public sector bodies will scarcely be in a position "to verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties". In addition to a lack of additional resources for public authorities, there is also a lack of:

- specific transparency and data security obligations for "public sector" or "responsible" bodies and further users of data,
- mandatory anonymisation for public sector bodies before they pass on data (without the consent of data subjects),
- guidelines on when data can be considered to have been anonymised reliably,
- a specific regulatory authority for such data transfers,
- clearly defined responsibilities of individual players,
- a low threshold for the legal protection of data subjects (the judicial process is still to be defined, but not recourse to administrative courts, arbitration board, etc.). This means that those affected will find it nearly impossible to defend themselves against violations of confidentiality obligations.

Furthermore, fair competition for small enterprises - for example, through greater regulation of large "data collectors" - is not an objective of the draft. Exclusivity agreements, which are permitted within a narrow framework, must therefore under no circumstances be concluded with large "data collectors". In this regard, orientation could be provided by the companies covered by the Digital Markets Act.

Finally, the added value of data sharing services, data cooperatives and "data altruism" organisations is unclear to workers, consumers or citizens. In view of the paltry rules on execution, concerns about deception and unconscionability predominate, brought about by the aggressive marketing of such services.

The AK's position

1. General remarks

On 25th November 2020 the European Commission published its proposal for a European Data Governance Act. This legal act regulates further commercial utilisation of data in the public sector which, based on data protection, intellectual property rights, or business secrets, are protected against access by third parties. It contains rules for the registration of companies that wish to utilise data jointly, for data intermediaries acting as a fiduciary between private individuals and data users, and for organisations which collect "donor data" "for the common good".

1.1 The preconditions for stimulating a data-driven economy are not satisfied

Politics, business and research are currently setting the course for the transition to a data-driven economy and unlocking the economic potential of data within the EU (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). This refers to data with and without personal reference and data from which personal reference has been removed, and which have thus been anonymised. Regarding the latter category, experts admit that algorithms can trace back almost any anonymisation through progressive machine learning. In other words: Consumers become re-identifiable. There is no statutory rule on when data can be considered to be non-traceably anonymised.

1.2 Making more data available" only if data protection is applied more forcefully

In its announcement on a European strategy for data, the European Commission emphasised that the European way is "to balance the flow and wide use of data while preserving high privacy, security, safety and ethical standards". In the opinion of AK, the trend towards a data economy is contrary to the principle of data minimisation (at least for personally identifiable or unreliably anonymised data). The need of artificial intelligence for more and more training data in the search for unknown patterns and correlations is often not compatible with the dictates of purpose limitation and privacy by design or default. The prospect is held out of a "both…and": of data economy and fundamental rights. This prospect is often not redeemable in reality. What is needed is an honest admission that sometimes there is only the "either… or" option: the commercial utilisation of large data pools for undefined purposes or a high level of data protection.

2. A closer look at the demands

The proposal does not clearly distinguish between data with or without personal references (and whether the data are sensitive, requiring special protection). However, the decision on whether the protective measures are sufficient is largely dependent on the category of data involved. This deficit can be found throughout the whole proposal. It must be clear when personal data are involved.

2.1 A clear separation between (non-personal and) personal data

The proposal does not clearly distinguish between data with or without personal references (and whether the data are sensitive, requiring special protection). However, the decision on whether the protective measures are sufficient is largely dependent on the category of data involved. This deficit can be found throughout the whole proposal. It must be clear when personal data are involved.

2.2 The duty to inform data subjects before data are passed on

Before data in the possession of public sector bodies are passed on to enterprises, all those affected must be informed by the public sector body of all important details. Only when they are informed that their data

will be passed on can they exercise their rights (information, objection, etc.).

2.3 A compliance agency with responsibilities clearly distinguishable from those of public sector bodies

Public sector bodies are not released from their obligation to maintain confidentiality (Art. 3(3)). However, "competent bodies" will be created (Art. 7) which will "support" the public sector bodies in the provision, anonymisation, etc., of data or which themselves are "entrusted" with granting access to data. This brings further players into the picture whose exact responsibilities are not clarified. Who is responsible for when and for what in the course of data transfer e.g. toGDPR, must be clearly defined in the proposal.

2.4 Clear allocation of responsibility between public sector bodies and re-users of data

Searching for the allocation of liability among all players in the event of a violation of data protection proves to be in vain. Data subjects can only defend themselves against inadmissible activities of authorities and commercial data users when they know against which party they can assert which claims.

2.5 Setting the bar low for legal protection

Any natural or legal person affected by a decision of a public sector body or of a competent body shall have the right to an effective judicial remedy before the courts (Art. 8(4)). This instruction is embedded in a provision which regulates the "single information points" and hence clearly refers to the low value placed on the rights of those affected. An information and independent arbitration point should be established for queries and complaints of interested or concerned citizens. In addition to legal redress before the courts, data subjects must also be able to lodge an objection against decisions under administrative law free of charge.

2.6 A regulatory authority as a controlling body over data transfer

The public sector body shall be able to verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information "jeopardising the rights and interests of third parties" (Art. 5(5)). Public sector bodies which have access to health, education, financial, mobility data, etc., are unlikely to be in a position administratively, legally, or technically, to control data processing conducted by enterprises. Even a competent body in accordance with Art. 7 can only offer support but has no regulatory role. An authority which can assume complex supervisory tasks is required.

2.7 Anonymisation of data to be performed exclusively by a public sector body

Public sector bodies may (Art. 5(3)) "impose an obligation to reuse only pre-processed data where such pre-processing aims to anonymize or pseudonymise personal data". Which player is to carry out anonymisation is not specified. In combination with Art. 5(4) (access by enterprises to data in a secure processing environment or on specific physical premises) there are grounds for concern that enterprises will be granted direct access to protected data in order to anonymise them themselves "in the secure processing environment" of a public sector body. AK is decidedly against this approach. Reliable data processing in accordance with fundamental rights presupposes that only anonymised data can cross the interface of the public sector body and data users can only access such data after anonymisation.

2.8 Prohibition of direct or remote access to protected data (without the consent of those affected)

In accordance with Art. 5(4) public sector bodies can restrict access to data so that access and reuse only take place "within a secure processing environment provided and controlled by the public sector" or "within the physical premises in which the secure processing environment is located". This discretionary clause must be replaced with explicit prohibitions. In the opinion of AK, public sector bodies should not allow direct or remote access to protected data without prior consent of those affected. In this case they must, without exception, transfer data in a condition that does not allow the data to be traced back to an individual.

2.9 Prohibition of the transfer of protected data to third countries outside the EU (without the consent of those affected)

In the opinion of AK Art. 5(10) must be removed without replacement. According to this provision, public sector bodies can only transfer confidential data to a re-user who wishes to transfer the data to a third country without a level of legal protection equal to the EU if certain contractual obligations have been entered into. However, in the opinion of AK, public sector bodies must not be allowed to cede protected data to third parties without the consent of the data

subject. If the data subject has given his or her consent to the reuse of his or her data, he or she must be able to decide freely whether he or she would like to consent to data transfer to a third country (in particular to a third country without a comparable level of legal protection).

2.10 A definition on when data can be considered to have been anonymised reliably

IT experts warn that the combination of ever greater data volumes and increasingly complex algorithmic data analyses mean that it can no longer be determined reliably whether data contain references to a person. EU citizens should be able to expect legal certainty with regard to the large-scale reuse of data. As part of the evaluation of "two years of the General Data Protection Regulation" many parties have pointed out this failure. When can data be considered to have been (sufficiently) anonymised? Which anonymisation methods are assumed to be a minimum standard? Should it be possible for no one (or only certain subjects) to trace data back to a uniquely identifiable person? In short: it remains to be clarified legally by whom, when, how and with what probability can allegedly anonymous data be traced back to an individual and therefore when can we speak (or not) of anonymous data.

For AK an "anonymisation law" is an essential prerequisite for access to sensitive data in accordance with fundamental rights:

- according to the GDPR the "principles of data protection should apply to any information concerning an identified or identifiable natural person. [...] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." It is therefore not a trivial matter of determining when a person can be identified. Numerous expert commentaries deal with drawing the line between anonymous and indirectly attributable personal data and often do not come to a unanimous conclusion. Furthermore, we wish to warn against the possibility that the development of deanonymisation methods could reveal a personal reference of formerly anonymous data.

- By way of illustration, we refer to the **experts' opinion prepared for the German Bundestag**: "How is the term of "traffic and utilisation data" used academically in a technical and legal context? How can this be distinguished from the term "metadata"?" According to this paper "the first step should be to clarify whether anyone can establish a personal reference. If it can be excluded objectively that the data subject can be identified, then there is no personal reference. However, a situation where not even a third party exists who can establish a personal reference is likely to be a relatively rare one. On the contrary, the ever-increasing variety of highly complex evaluation mechanisms and their ready availability actually increase the number of bodies in a position to establish a personal reference between stored data and a natural person. In this regard it is of equal importance that the quantity of data is increasing and the demand for such is increasing likewise."

- As long as traceability cannot be excluded objectively because a third party can establish a personal reference, according to the CJEU, it is a question of the means which can be used to establish a personal reference. Specifically, in the case of Breyer (C-582/14) the judges asked the question whether the responsible body had access to reasonable means in order to obtain the necessary information from third parties in order to attribute the data. In their opinion, it is not expressly a question of whether "all the information enabling the identification of the data subject is in the hands [of the party responsible for the data]". The CJEU did not clarify in this context what "reasonable means" are. The court merely gave a negative definition: "Means which cannot reasonably be used and which therefore must be disregarded in determining a personal reference are those whose utilisation for identification is prohibited by law or with which identification cannot practicably be carried out."

- The current government agreement of the Austrian Federal Government has also undertaken to determine criteria for reliable anonymisation of data.

2.11 Considering the risk of the re-identification of persons using anonymised data

This requirement in Art. 5(11) incomprehensibly refers only to data transfers to third countries. Precautionary measures and limitations against the illegal reversal of anonymisation must of course also be taken when data circulate within the EU.

2.12 Specifying how the most important principles of the GDPR are to be applied to data transfers

A brief reference to the fact that the proposal does not affect the GDPR is by no means sufficient. Tailor-made data protection and data security measures which are appropriate to combat the risk of data transfers between public sector bodies and enterprises are missing. The proposal should establish how the most important GDPR principles can be harmonised with access rights. This includes: data minimisation, requirement for consent to data utilisation in the knowledge of the exact purposes of processing, a prohibition of further processing for purposes not compatible with the original purpose, etc.

In any event, the GDPR establishes narrow limits for the reuse of personal data. Normally, only reliably anonymised data should end up in the data pool for further processing to develop innovative business ideas. In accordance with Art. 5(6) public sector bodies should support potential data users in seeking consent. The distribution of roles must be clarified in the proposal: who informs who in accordance with Art. 12 et seq. GDPR, who provides information in accordance with Art. 15 GDPR, who records which processes and receives retractions of previously given consent?

2.13 An obligation for data protection authorities to carry out prior checks for applications subject to impact assessment under the GDPR

Data subjects want precautions to be taken instead of finding themselves at a disadvantage afterwards and merely being able to claim damages. In order to meet the clear call from experts for a prior check of the "fairness" of algorithms, more official inspections will in any case be required in the future prior to any risky applications. What is strictly necessary for automated individual decisions in the future should apply to all data processing operations that require an impact assessment. In this way, violations of fundamental rights can be prevented even before they cause damage.

2.14 Clear rules for providers of data sharing services

Art. 9 stipulates a notification procedure for the activity of a data sharing service. These are intended as intermediation services between "data subjects that seek to make their personal data available" and potential data users. A vague reference is made to the GDPR. Which services a data sharing service should provide vis-à-vis consumers as the minimum contractual content remains open. Nor can it be deduced from the requirements of Art. 11 concerning protection against fraud, abuse, data protection and security what consumers can commission data sharing services to do. Added value would be provided by establishing the conformity with the GDPR of services which the consumer wishes to use and, failing which, the legal remedy; this to be included in the minimum contractual content. Ultimately, this is a task for lawyers and hence is nothing significantly new.

2.15 Clear rules for data cooperatives

These must also be registered, negotiate the conditions for data processing which are "supporting data subjects"…"to negotiate terms and conditions for data processing before they consent…and allowing for mechanisms to exchange views…that would best represent the interests of data subjects". How such a group is to come to legally binding decisions is beyond imagination. Apart from an impenetrable definition of the term, the text is not illuminating.

2.16 Clear allocation of the tasks of regulatory authorities

A variety of authorities are responsible for data sharing services and data cooperatives: the authority for registration, data protection, national competition, cybersecurity and other "relevant sectorial authorities" (Art. 12 and 13). The proposal does not clarify exactly who is responsible for what.

2.17 More protection vis-à-vis "data altruism organisations"

Apart from mandatory registration (including its possible cancellation) there are few protective measures against the danger of unconscionability and exploitation of the credulousness of consumers. In accordance with Art. 19, data holders in registered organisations must be informed "about the purposes of general interest" and "any processing outside the Union". Such fragments of information do not satisfy the GDPR requirements for information and consent. Measures must be taken to ensure that aggressive, misleading marketing practices (e.g. surreptitiously obtaining medical data for the putative object of helping the sick, promises of prizes, etc.) are not used to canvass data donors. These types of organisations should be treated exactly the same as commercial data sharing services. Furthermore, sanctions imposable by administrative authorities should be included if the body falsely claims to be a recognised data altruism organisation.

Contact us!

In Vienna:

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