AK EUROPA

Position Paper
April 2022
Consumers

COM(2022) 68

Data Act

Significantly more consumer protection for the Internet of Things

Executive summary

What does it involve?

The draft regulation aims to make data generated by internet-connected devices available to many stakeholders – the users of the products, the so-called "data holder" (manufacturer, seller, lessor or other authorised party), authorised third parties, public bodies, and science and research in the public interest. This is not intended to affect the General Data Protection Regulation (GDPR) and the e-Privacy Directive.

Under the Data Act, consumers have the right

- to be informed about the accumulation of data,
- and obtain (as direct as possible) access to this data themselves and
- to also provide third parties with data access at their request.

Summarised AK assessment

The explosive nature of the project becomes apparent as soon as the rules proposed by the EU Commission are applied and not only to visionary areas such as autonomous driving cars or smart homes. Due to its general wording ("data generated by the use of a product or related service"), the regulation might also apply to millions of everyday devices and services such as digital TVs, eBook readers, voice assistants, fitness trackers, and many more. With smart devices (Internet of Things, IoT), consumers run the risk of being exposed to excessive commercial monitoring of their everyday behaviour, profiling, and behavioural manipulation (through targeted offers, advertising, personalised pricing), just as with internet surfing. Our privacy is also coming under pressure when we drive our cars, brush our teeth, heat our homes, play sports, watch TV, or play games. It is therefore essential to strengthen consumers' digital sovereignty over the data generated during device and service use!

After all, what would remain private if TVs and robot vacuum cleaners constantly suck up usage data and third parties know exactly when and what Person X is watching, where and when he/she is at home, and how big the apartment is?

The interests of the data economy have a blatant priority over the digital sovereignty of consumers. With its Data Act, the EU Commission is pursuing the goal of "ensuring fairness in the allocation of value from data amongst actors in the data economy and to foster access to and use of data". The Data Act does not live up to the EU Commission's own claim to "balance the flow and use of data whilst preserving high privacy, security, safety, and ethical standards". This is because, for long stretches, it does not deal with these protected goods, which are important for consumers, but rather primarily with the protection of SMEs and non-discriminatory access conditions for third parties to data.

AK's position paper on the Internet of Things raised awareness many years ago of the danger of erosion of (fundamental) consumer rights in networked goods and recommended protective measures. In view of the implications of the Data Act for society as a whole, AK considers it to be appropriate to go back to the start in order to make up for what has been missed: Consumer and data protection expertise (EDPD, EDPS, BEUC, university civil law institutes) should be involved in the drafting process from the beginning to better balance the rights and obligations of stakeholders. Amongst the most essential concerns are:

- Digital self-determination of consumers/citizens
- Right to be Offline

AK's position

Background

Monitoring risks

E-book readers and networked TV sets send data on user behaviour to companies, fitness wristbands measure the pulse and supply health data to third parties, remote controls in smart homes preheat the oven and monitoring boxes in the car transmit driving behaviour to insurance companies, all of which makes the amount of premium payments dependent on the measured data. 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. It does not help that Art 6 restricts the use of data by third parties commissioned by the user (profiling ban). The provisions do not apply to the data owner and third parties commissioned by him/her.

Data protection

The draft Data Act grants data use rights to various stakeholders. No distinction is made between personal and non-personal data – a fundamental error. In view of completely different legal consequences, it is not appropriate to speak of data in general terms. Only in the case of data without any personal reference can the EU Commission grant consumers a mere right to participation.

Their announcement: "We want to give consumers and businesses even more say over what can happen to their data by clarifying who has access to it and under what conditions," is downright misleading in light of the fact that most data is subject to processing restrictions or bans.

Business models

Networked products have a strong service component. Instead of a classic purchase with complete transfer of ownership (also with regard to digital components), only rights of use are granted, as is the case with works protected by copyright, which the provider can structure as he sees fit. There is a need for legal action against the emerging imbalance of rights and obligations of the contracting parties, which the draft does not address (the Data Act only prohibits unfair contract clauses to protect SMEs).

Holders can exclude third parties from accessing their property. If they are only licence users, the data economy can unilaterally dictate online compulsion and surveillance methods to them. Consumers will then no longer decide autonomously how anonymously they use devices. EC 20 explains that smart device users "typically have to register and are given an individual account". The right to continue to use household appliances anonymously must be strengthened. Users are also subject to controls and prohibitions if they wish to modify the item, repair it themselves, or have it repaired. Consumer ownership of the entire product would need to be clarified.

Online constraint

With the Internet of Things in children's toys, surveillance practices have also arrived in children's rooms. Very young children were able to gain their first experience with commercial confidentiality violations, for example with the Cayla doll. Conversations could be passed on to US manufacturer via Bluetooth connection, microphone, and voice recognition. Problems associated with online games in general are: hidden recording of behaviour and non-transparency of data recipients and purposes of data use. Many games have to be played online, even when one person alone plays the game and an internet connection is not required. This pressure to be "always-on" is likely to increase. Without a right to be offline that is expressly incorporated, consumers will only have the choice of take it or leave it (see AK study)

In summary, a glaring imbalance is emerging in the legal positions between providers and their customers. The supply side

- uses contractual and technical means to analyse personal customer data and operating data and exploit them commercially;
- assumes little responsibility (to ensure quality levels, liability in the event of damage, warranties for defects) for inherent IoT risks (software failures, hacking attacks, data breaches, insolvencies of involved providers, damaging use of immature algorithms and artificial intelligence) and does not invest in preventive security;
- weakens consumers' position because ownership rights deriving from a purchase and relating to individual components are undermined with increasing frequency and replaced with simple rights of use under copyright;
- monitors consumers moving through a densely networked everyday life. Every point of contact with smart devices leaves traces of personal data, which can end in comprehensive utilisation and location profiles. The development of monitoring everyday actions, which began with the tracking of PC and mobile phone users, takes on a new dimension with IoT. The interfaces with the Internet, where consumer behaviour can be observed, evaluated, and transmitted to third parties, are increasing, providing a uniquely accurate picture of what we do, what we don't do, what we think, who we are in contact with, and much more;
- exposes consumers to safety risks: In the race to bring innovative products to market faster than the competition, very badly designed appliances end up in households. Furthermore, it is accepted that, due to the system, software can never be completely error-free. Security updates bear witness to this situation. What consumers can be expected to put up with or not in terms of development risks, a lack of readiness for market, and a lack of security measures against malware, data breaches, and hacking attacks, is at best at the discussion stage. There is a danger that consumers will be used as "guinea pigs" by products that are unsafe from a technical or data protection point of view. Often, investments in product and data security are only made reactively after mishaps with significant consequences (and media coverage) have already occurred;

AK sees the following need for improvement

Digital self-determination of consumers/citizens

Fairness rules and arbitration bodies are only provided for by the Data Act for disputes between companies involved in the flow of data. The draft does not address consumer needs and their legal protection interests (with the exception of a right to information, data access and "data sharing"). Consumers who buy products are regarded in the draft as "users" (instead of owners with sole rights of disposal). Consumers do not have a secure right to use their product offline or to restrict data generation. They (in contrast to SMEs) do not enjoy any protection (beyond Directive 93/13/EC) against IoT-specific unfair contract terms. It is unclear whether they can resell their individualised product or repair it themselves. It is also unacceptable that the obligations of data recipients under Art 6 (e.g. no manipulation and behavioural profiling of users) do not apply to the data controller.

Right to be Offline

Users have a strong interest in having the option to switch off networked functions and still use the main functions of the product offline. Manufacturers and service providers have conflicting interests (know your customer, more profit through networked additional services, sales of data). Thus, the right to be able to deactivate internet connections – without losing core functions of the device – must be legally secured. The importance of this offline right is shown by the insistence of many consumers on a switch-off function for smart meters and digital electricity meters.

Coherent Scope

Home equipment, consumer goods, and virtual assistants are covered (Recital 14 and 22), but "equipment primarily intended for playing content, such as PCs, servers, mobile phones, cameras" are not. Why Siri, Alexa, and presumably smart TVs, which are also content providers, are included in the Act, but smartphones are not, seems extremely arbitrary. In any case, the latter should fall within the scope.

Clarify roles and responsibilities

It is not clear from the draft who is the so-called data holder amongst several possible parties (manufacturer, additional service provider, software supplier, seller, other third parties). It is unclear from which EU provisions the role of the data holders can be derived beyond doubt by definition and which

authorisations are associated with it. The same applies to the question of who has to fulfil which obligations to consumers. Roles and associated responsibilities must be identified clearly in the draft in a legally sound manner.

Clarify personal reference

The Data Act applies equally to personal data and non-personal data. That the provisions do not distinguish between types of data is a conceptual flaw. What may be harmless in one case may be a serious violation of fundamental rights in another. Incidentally, many researchers believe that device data usually have an (indirect) personal reference that is protected by fundamental rights. To speak indiscriminately of "data" can thus be a calculation: in practice, the data economy will often unreflectively invoke rights of use, which conflicts with the GDPR. Data protection authorities, already stretched far beyond their limits, are unable to check this on a regular basis. It does not help that, according to Recital 5, it is not intended to create new legal bases for data processing with the Regulation. For other data, a right of information, access, and "data sharing" may be sufficient. According to the GDPR, on the other hand, principles such as data minimisation must be observed and data use without a legal basis is prohibited. The EU Court of Justice's case law on the GDPR is making extremely slow progress. The data economy benefits from the legal uncertainty as to whether or not there is personal reference in an individual case.

Balancing fundamental rights for data access in emergencies

The draft also does not dwell long on fundamental rights barriers: public bodies, but also ominous (because undefined) agencies and institutions, can request data if there is an "extraordinary need" that is not defined in more detail regarding the fulfilment of public interests in an emergency. Icebreaker in favour of population data analysis is undoubtedly the mass analysis of mobile operator data to manage the current pandemic better. However, the Data Act's permission to interfere with citizens' privacy is so vague that sensitive device data could be accessed even in the case of less weighty public interests and emergencies.

No protection gaps due to exceptions for SMEs, which would not have to observe consumers' right to information, access, and "sharing" of data according to the draft.

With regard to contract law, consumers must also...

- be able to make their own decisions about what to do with the product they have purchased in every respect;
- have ownership of the product with all built-in software components;
- have an unrestricted right of self-determination over all data generated by the product;
- be able to decide freely about whether and to whom they make those data available;
- be able to choose their repair shops and service providers freely in every respect and they must not be forced to accept tie-in contracts;
- be confident that the manufacturer/seller will not cite liability or warranty disclaimers if the consumer takes the device to a repair shop of his/her choice or does not make available all the data that has been generated
- are also allowed to repair devices themselves and
- have a right of choice (products must have smart functions that can be deactivated).

On the details of the Commission's draft

Art 1

The full harmonisation character is detrimental to legal certainty. Like other regulations relevant to fundamental rights (GDPR, DGA), the provisions are too general to regulate complex issues with legal certainty. Sector-specific specifications are needed so that addressees of the norm are not faced with countless questions of interpretation that have to be clarified in court. Since the draft also grants rights and obligations to public bodies (or agencies or institutions acting in the public interest, which are not defined in more detail), it must be remembered that they are subject to the same rights and obligations under the Austrian Federal Constitution Act. In accordance with Art 18 of the Austrian Federal Constitution (principle of legality and certainty), the government can only act on the basis of sufficiently defined laws.

The scope of application refers to both personal data according to the GDPR and data without personal reference. A conceptual error: a separation must be made and criteria used to determine when a reference to a person is deemed to exist. One-size-fits-all rules do not meet the different needs of protected persons (consumers as data subjects or companies as owners of intellectual property rights) and different risks.

Art 2

The definition of "data holder" is far too vague: The data holder would be anyone who has the right or obligation (under the Data Act or other EU law) to make certain data available. The vague definition leaves open who exactly has to inform consumers and who has to react to access and data sharing requests. The term "data holder" is also inappropriate: there are no ownership or property rights when it comes to inalienable personal rights. The GDPR also considers this by stipulating that consent to data use must always be revocable. In this respect, it would be more accurate to speak of data controllers under the GDPR, who may use personal data in compliance with Art 5 et seq. of the GDPR, and rights holders to other, non-personal data based on corresponding agreements or statutory provisions. This distinction should run through the entire draft, but it does not – to the detriment of legal certainty and consumers.

The definition "user" weakens the position of buyers: A user should be someone who owns, rents, or leases a product. What legal position this person has with regard to (non-) personal data is unclear and in urgent need of regulation. Owners can freely decide, for example, to use products offline, to exclude third parties from accessing products, etc. A right of use is not a right of disposal comparable to ownership!

Art 3

Clarify obligation addressees: The draft consistently avoids naming the obligation addressees. "Products shall be designed..." might be directed at the manufacturer. Nevertheless, who has to implement the following provision: „Before concluding a contract at least the following information shall be provided"? This vagueness is therefore unacceptable because the definition of the data holder also leaves room for speculation. If the role of the data holder is to be derived from EU law, consumers should also find out from which legal provisions this can be derived in individual cases. According to Art 3(2) (e), the data controller may be "the seller, renter or lessor" or someone else entirely (the manufacturer of the product would be the obvious choice). Art 3(2)(d) compels (whoever) to clarify whether the manufacturer supporting the product or the provider of ancillary services intend to use data themselves or allow third parties to do so. This mishmash of unclear roles and responsibilities needs a thorough overhaul.

The provision contains some useful information obligations towards consumers. However, it should be supplemented with...

- instructions on how to restrict or disable data generation.
- information on which independent arbitration body consumers can call on to clarify questions/ complaints about the legally compliant implementation of the Regulation and to enforce their rights.
- the requirement that the information obligations under Art 3 are to be fulfilled in a clearly visible manner and together with those of the GDPR (Art 12 to 14). The information must also be found on product packaging.

Rectification of the "By Default" obligation: It is welcomed that the provision practically prohibits proprietary/self-contained systems. Open standards are needed to enable data sharing with third parties. However, it is unclear how the "By Default" principle is to be implemented in concrete terms in the manufacture of products. According to the provision, the product design should provide the product user with easy access to data. At the very least, examples should be given of what exactly is covered by this obligation. Since "By Default" usually means consumer-friendly default settings, it should be clarified whether and which selection options consumers have to find. The core demands of AK are that

- products are to be constructed "by design" in such a way that they can be optionally used offline in a simple manner,
- products are clearly marked for buyers if their use requires online connections due to technically compelling requirements for their basic use.
- a ban on mandatory always-on is established: outside operating hours, consumers must be able to easily deactivate the Internet connection and data generation even for products that can only be used online (contrary to Recital 17).
- non-personal data (in analogy to the GDPR) can be regulated in a data-saving manner via settings. This is because the question of when an indirect reference to a person exists is highly controversial. In case of doubt, the buyer of a product must be able to stop any data flow that is not necessary for the basic use of a product.

Art 4

Direct access right of the user to the data: The provision is providing for users the right of access should the data not be directly accessible. Art 3, on the other hand, provides that data must be "easily, securely, and where relevant and appropriate, directly accessible to users". It does not provide clarification regarding when direct data access is not "relevant

and appropriate". If operational data can be easily generated and utilised, it is in principle also reasonable for manufacturers and software suppliers to set up an interface for direct consumer data access. Where it is technically impossible or disproportionate in terms of cost, the Regulation should explain in more detail and require regulatory authorities to monitor the market accordingly.

Evidence in compliance with the GDPR:
In the case of personal data, it must be pointed out that the information obligations pursuant to Art 13-14 GDPR must be complied with, without the data subject having to identify him/herself beforehand. Only in the case of the right to information under Art 15 may clarification of the data subject status be necessary under certain circumstances. In Art 4, it is therefore essential to distinguish between (non-) personal data.

Priority of transparency over trade secrets:
Buyers need meaningful information before they buy (to make an informed decision for or against a product) and during use (to control the flow of data and change it if necessary) of a product. Trade secrets must not stand in the way of the need for transparency.

Art 5

Fair contracts between "data holder" and "user":
Whilst quite a few provisions are dedicated to the imbalance of power in the B2B-sector and unfair B2B-terms and conditions, this is completely missing with regard to consumers. It is merely standardised that non-personal data may only be used based on contractual agreements. The data owner may not use the data to gain insight into the economic situation, production methods, or commercial data use of a user. The protection addressees are commercial users who fear that their operational situation will be spied upon. Where are the protections for users who are consumers? Forgetting about their need for protection in unfair contracts is unacceptable.

Art 6

Many operational data are subject to the GDPR.
There is a need for a sector-specific directive for the handling of personal data in IoT products. The GDPR is too general in providing information about when third parties (but also the completely unregulated data holders) may store user data and use it for different purposes. When is consent required? When can legitimate interests be asserted? What security measures are required? The regulation does not clarify these questions, nor does the GDPR provide any answers. Consumers cannot be expected to wait years for court or official decisions on basic questions about IoT products. Furthermore, we see that in individual cases Member States give completely heterogeneous answers to questions of interpretation of the GDPR. Against this background, an IoT Data Protection Directive is needed to protect against legal uncertainties and excessive data use.

The requirements for third parties (e.g. prohibition of dark patterns or profiling not necessary for service provision) are welcomed but should apply to the data controller as well. It is not acceptable that the latter does not have to comply with the same fairness rules.

Art 7

Unobjective exemption of SMEs from the obligations in Chapter 2:
Whether small or large, the rules for the exploitation of data must aim at transparency, fairness, and basic protection of fundamental rights and must be complied with by every economic enterprise. The exception is factually unfounded, exposes consumers to unnecessary risks, and worsens their legal position and informational situation. Against this background, Art 7 should be deleted.

Art 10

Dispute resolution not only for B2B-conflicts:
Data holders and data recipients can settle their disputes before an independent dispute resolution body. Such a low-threshold system should also be open to consumers. One of the difficult to understand deficiencies of the draft is to only consider B2B-conflicts.

Art 11

Sanctions are missing:
Ending unauthorised access to data and deleting the improperly stored data cannot be the only consequence of data misuse. Since the Regulation – as emphasised repeatedly – does not distinguish between (non-) personal data, reference must be made to the GDPR (e.g. data breach notification, sanctions). Similar measures should apply to – often only allegedly – non-personal data in order to keep cases of misuse to a minimum by imposing reasonably deterrent sanctions. The exemption provisions only focus on the situation of the data holder (no significant harm, disproportionality) and once again forget about the consumers who are at least equally affected.

Art 13

Unfair T&Cs towards SMEs:
There are no protective provisions in consumer law (other than the requirements of Directive 93/13/EC) that specifically address the contractual risks of IoT. The fact that SMEs are considered worthy of protection, whilst consumers are not, is not factually comprehensible.

Chapter 5

Access by public authorities may not comply with fundamental rights:
The provisions of the chapter are too vague to constitute a direct legal basis for the action of public authorities, which may act only pursuant to precisely worded statutory orders. If the provisions were only aimed at the data holder's obligations to surrender data, it would have to be explicitly stated that these only apply if a sufficiently specific authorisation by the authorities is enshrined in national or EU law. Shortcomings of the chapter include that:

- Not only public bodies, but also "agencies and bodies acting in the public interest" can request the surrender of personal data "in case of exceptional need" (exception: security police tasks). The basic requirements for a reasonably legally secure standard are not met. Who, what, when, and how it is allowed, remains unclear to a high degree. Eligible agencies and entities are defined no further. What need must there be for interference with the constitutionally protected rights to data protection and privacy?

- In any case, the scope of this provision is enormous. Every smart car is subject to the scope of the Regulation, which means that all personal location data could also be analysed by public authorities claiming a specific need. However, millions of users' data cannot be accessed seriously without a court order. Art 17 states that – as far as possible – non-personal data should be requested and Art 18 states that "reasonable efforts should be made to pseudonymise the requested data". The latter, however, only if the purpose of the query can be fulfilled with pseudonymised data.

Due to its disproportionate level of interference with the fundamental rights of the population, the chapter needs to be revised thoroughly under inclusion of the EU Data Protection Supervisor and EU Data Protection Committee.

Contact Us!

In Vienna:

Daniela Zimmer
T +43 (1) 501 65 1
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 (2) 230 62 54
alice.wagner@akwien.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.