Positioning Free ICT Europe - Free Flow of Data

Machine-generated data is created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real. An example can be performance data and error-codes.

To stimulate Innovation, to be able to improve services & processes and the development of new business models full access to Machine Produced Data (MPD) is required. Though not only the access to the data; when the data are 'codes' you should be able to transfer a code to an explanation/value of this specific code.

Access to Machine Produced Data is also identified by us as an important element in serviceability and repair.

The EU Commission signed Circular economy and Sustainability agreements, this leads to put more focus on serviceability, reparability and extending life cycle of products/equipment in several EU workgroups (Ecodesign, WEEE directive, IoT project group). Also the EP recent accepted a report which is a vote to a.o. increase durability, open up the repair market and demand manufacturers to provide Software/Data.

Free ICT Europe trusts these developments will be incorporated in the decision process about the Free Flow of Data.

Our positioning:

Machine Produced Data (data, performance data, logs) should be accessible, for accurate diagnostics for example.

- To develop an API, Manufacturers should provide:
    - Mapping instructions for the data and the interpretation tables (and provide updates when the occur)
    - Updates on mapping and interpretation
    - A (downloadable) data set for testing purposes
- When the manufacturer has a tool available (might be password protected): access to this tool to read the data and interpretation should be given without restrictions and without additional contracts;
- The owner/user should be able to share the MPD with partners they select;
- The owner/user should be able to block (the automatically) sharing of the MPD with the manufacturer;

Relevant text from the Free Flow of Data Working Document :

3.3. Raw machine-generated data: Legal situation at EU and national level

Raw machine-generated data are not protected by existing intellectual property rights since they are deemed not to be the result of an intellectual effort and/or have any degree of originality. The sui generis right of the Database Directive (96/9/EC) – which gives makers of databases the right to prevent extraction and/or reutilisation of the whole or of a substantial part of the contents of a database – may provide protection only under the condition that the creation of such a database involves substantial investment in the obtaining, verification or presentation of its contents.

The recently adopted Trade Secrets Protection Directive (2016/943/EU), to be transposed into national law by June 2018, will grant protection to trade secrets against their unlawful acquisition, use and disclosure. For data to qualify as a "trade secret", measures have to be taken to protect the secrecy of information, which represents the 'intellectual capital of the company".

Under the law of different Member States, legal claims are applied to data only when that data meets specific conditions for it to qualify, for instance, as an intellectual property right, database right or a trade secret. However, as at EU level, raw machine-generated data as such would not generally meet the relevant conditions.

Therefore, comprehensive policy frameworks do not currently exist at national or Union level in relation to raw machine-generated data which does not qualify as personal data, or to the conditions of their economic exploitation and tradability. The issue is largely left to contractual solutions. The use of existing general contract law and competition law instruments available in the Union might be a sufficient response. In addition, voluntary or umbrella agreements covering certain sectors might be envisaged. Nevertheless, where the negotiation power of the different market participants is unequal, market-based solutions alone might not be sufficient to ensure fair and innovation-friendly results, facilitate easy access for new market entrants and avoid lock-in situations.

3.4. Situation in practice

In some cases manufacturers or service providers may become the de facto "owners" of the data that their machines or processes generate, even if those machines are owned by the user. A de facto control of this data can be a source of differentiation and competitive advantage for manufacturers. However, this can be problematic, because the user is often prevented by the manufacturer from authorising usage of the data by another party.

The different market players that are in control of the data, depending on the specificities of the markets, may thus take advantage of gaps in the regulatory framework, or of the legal uncertainties described above, by imposing unfair standard contract terms on the users or through technical means, such as proprietary formats or encryption. While several Member States have extended the scope of application of the consumer protection Directive on Unfair Contract Terms also to B2B transactions, not all have done so. This could result for instance in users and businesses becoming locked into exclusive data exploitation arrangements. Voluntary data sharing might emerge, but negotiating such contracts could entail substantial transaction costs for the weaker parties, when there is an unequal negotiation position or because of the significant costs of hiring legal expertise.

Ensuring access to machine-generated data is currently being explored by some Member States, which may decide to regulate this issue by themselves. An uncoordinated approach risks creating fragmentation and would be detrimental to the development of the EU data economy and the operation of cross-border data services and technologies in the internal market.

Accordingly, the Commission intends to engage in a dialogue with Member States and other stakeholders to explore a possible future EU framework for data access. In the Commission's view, this dialogue should revolve around the most effective ways to achieve the following objectives:

* **Improve access to anonymous machine-generated data:** Through sharing, reuse and aggregation, machine-generated data becomes a source of valuecreation, innovation and diversity of business models.

* **Facilitate and incentivise the sharing of such data**: Any future solution should foster effective access to data, taking into account, for example, possible differences in bargaining power between market players.

* **Protect investments and assets:** Any future solution should also take into account the legitimate interests of market players that invest in product development, ensure a fair return on their investments and thereby contribute to innovation. At the same time, any future solution should ensure a fair sharing of benefits between data holders (*The entity that manages and retains the machine-generated data in practice)*, processors and application providers within value chains.

* **Avoid disclosure of confidential data**: Any future solution should mitigate the risks of disclosing confidential data, in particular to existing or potential competitors. In this regard it should also allow for proper data classification to be performed, prior to the assessment of whether or not a certain piece of data can be shared.

* **Minimise lock-in effects:** The unequal bargaining power of companies and private individuals should be taken into account. Lock-in situations, especially for SMEs and startups and private individuals, should be avoided.

In the stakeholder dialogues, the Commission intends to discuss the following possibilities for addressing the issue of access to machine-generated data, which differ in their level of intervention:

* Guidance on incentivising businesses to share data: To mitigate the effects of divergent national regulations and provide increased legal certainty for companies, the Commission could issue guidance on how non-personal data control rights should be addressed in contracts. This guidance would be based on existing legislation, in particular the transparency and fairness requirements laid

down by EU marketing and consumer law, the Trade Secrets Directive and copyright legislation, notably the Database Directive. The Commission intends to launch an evaluation of the Database Directive in 2017.

* Fostering the development of technical solutions for reliable identification and exchange of data: Traceability and clear identification of data sources are a precondition for real control of data in the market. The definition of reliable and possibly standardised protocols for persistent identification of data sources can be necessary to create trust in the system. Application Programming Interfaces (APIs) can also foster the creation of an ecosystem of application and algorithm developers interested in the data held by companies. APIs can help firms and public authorities to identify, and profit from, different types of re-uses of the data they hold. On this basis, broader use of open, standardised and well-documented APIs could be considered, through technical guidance, including identification and spreading of best practice for companies and public sector bodies. This could include making data available in machine-readable formats and the provision of associated meta-data.

* Default contract rules: Default rules could describe a benchmark balanced solution for contracts relating to data, taking due account also of the ongoing Fitness Check on the overall functioning of the Unfair Contract Terms Directive. They could be coupled with introducing an unfairness control in B2B contractual relationships27 which would result in invalidating contractual clauses that deviate excessively from the default rules. They could also be complemented by a set of recommended standard contract terms designed by stakeholders. This approach could lower legal barriers for small businesses and reduce the imbalance in bargaining positions, while still allowing a large degree of contractual freedom.

* Access for public interest and scientific purposes: Public authorities could be granted access to data where this would be in the "general interest" and would considerably improve the functioning of the public sector, for example, access for statistical offices to business data, or the optimisation of traffic management systems on the basis of real-time data from private vehicles. Access to business data by statistical authorities would typically contribute to alleviating the
27. Obviously the benchmark for the unfairness level for B2B would need to be different from B2C contracts, as to reflect the higher degree of contractual freedom in B2B relationships.

statistical reporting burden on economic operators. Similarly, access to and the ability to combine data from different sources is critical for scientific research in fields such as medical, social and environmental sciences.

* Data producer's right: A right to use and authorise the use of non-personal data could be granted to the "data producer", i.e. the owner or long-term user (i.e. the lessee) of the device. This approach would aim at clarifying the legal situation and giving more choice to the data producer, by opening up the possibility for users to utilise their data and thereby contribute to unlocking machine-generated data. However, the relevant exceptions would need to be clearly specified, in particular the provision of non-exclusive access to the data by the manufacturer or by public authorities, for example for traffic management or environmental reasons. Where personal data are concerned, the

individual will retain his right to withdraw his consent at any time after authorising the use. Personal data would need to be rendered anonymous in such a manner that the individual is not or no longer identifiable, before its further use may be authorised by the other party. Indeed, the GDPR continues to apply to any personal data (whether machine generated or otherwise) until that data has been anonymised.

* Access against remuneration: A framework potentially based on certain key principles, such as fair, reasonable and non-discriminatory (FRAND) terms, could be developed for data holders, such as manufacturers, service providers or other parties, to provide access to the data they hold against remuneration after anonymisation. Relevant legitimate interests, as well as the need to protect trade secrets, would need to be taken into account. The consideration of different access regimes for different sectors and/or business models could also be envisaged in order to take into account the specificities of each industry. For instance, in some cases, open access to data (full or partial) could be the preferred choice both for firms and for society.