Meeting with [Name] at Uber

[Redacted Text]

[Redacted Text]
LTT
(on Platform Work Directive)

- The GDPR provides for **a general framework for the protection of personal data, including rules on data subjects’ rights**. These rights are particularly relevant for people working through platforms subject to algorithmic management. However, it was considered necessary to complement and specify certain GDPR rules in the context of platform work in order to address **problems specific to this work**, including in particular the lack of transparency and clarity of rules concerning the use of algorithmic management.

- The Commission proposal aims at **promoting fairness, transparency and accountability** in algorithmic management in the platform work.

- To this end, the proposal provides for instance rules on:
  
  o the platforms’ obligation to inform platform workers on the existence of an automated monitoring and decision-making system, as well as on how and for what purposes such systems are used;
  o the prohibition on the processing of certain personal data which is not connected to and necessary for the performance of the platform work;
  o the platform workers’ right to a human review of certain decisions taken or supported by an automated decision-making system and the modalities of such review.

- The proposed rules **complement and specify GDPR rules** concerning, in particular, the data controller’s information obligations (Article 13 and 14 GDPR) and the requirements concerning decisions based on automated processing (Article 22 GDPR). Where no more specific rules are provided, GDPR rules continue to apply.
The proposed rules are fully in line with the GDPR as they clarify further the data protection rights of platform workers and the respective obligations of platforms. These rules allow platforms to continue the use of algorithmic management and process personal data in this context as long as such use is transparent and limited to what is strictly necessary, and provided that necessary data protection safeguards are in place.

(on AI Act, in general)

- The AI Act is a product safety legislation; at the same time is fundamental rights aware.
- The AI Act follows a risk-based approach. We identified high risks in areas such as education, employment, access to credits or public assistance benefits, law enforcement, migration and asylum, as well as the justice systems and remote biometrics systems like facial recognition applications. We ban certain applications where we deem the risk unacceptable for our EU values., such as systems used for social scoring by public authorities.
- The proposal will help to ensure that high-risk AI systems are designed in a fundamental rights compliant way. The new requirements will protect against challenges, such as the complexity and opacity of certain AI applications (black box effect), bias and discrimination. The new requirements will ensure that possible breaches of fundamental rights obligations can be investigated and addressed by national authorities and courts.
- To achieve this, the proposal includes requirements on the reliability and accuracy of the systems, appropriate documentation and testing of high-risk AI applications, as well as adequate human oversight.
- The users of AI systems are the ones who need to respect fundamental rights, so they need adequate information from the providers. This is regulated in the proposal.

(on AI Act & data protection)

- EU data protection rules remain fully applicable. For example: The fact that an AI system is classified as high risk under this Regulation and can be put into market, should not be interpreted as indicating that the use of the system is necessarily lawful under other Union law or under national law, such as on the protection of personal data. The AI system must comply also with EU data protection law.
• The AI Act, in certain cases, specifies the EU data protection rules and is fully in line with them. This is the case with regard to the processing of sensitive personal data, the processing of personal data in the context of regulatory sandboxes and finally the use of real-time remote biometric identification systems in the law enforcement area.
  o To this end: The AI Act provides for the legal basis of processing of sensitive personal data, where such processing is strictly necessary for the purpose of ensuring bias monitoring, detection and correction during the development of AI systems.
  o Moreover, the AI Act provides for the legal basis for further processing of personal data in the regulatory sandboxes as regards the areas of public safety and health (including disease prevention, control, treatment) and the improvement of the quality of the environment.
  o It also provides for rules for the processing of personal data in the sandbox, such as the obligation to delete the data when the AI system leaves the sandbox.
  o In the law enforcement area the AI Act frames the narrow exceptions under which real-time remote biometric identification systems may be used. It also frames the establishment of regulatory sandboxes in the area of law enforcement. In addition, the AI Act requires a national law authorising such usages in the law enforcement area.

• The AI Act reinforces the data protection rules. This is the case with regard to users’ obligations and the role of the DPAs in the AI Act.
  o The AI Act establishes the obligation of the user of high-risk systems to use the AI system providers’ information for conducting the data protection impact assessment (DPIA), for instance information on the level of accuracy of the system, the specifications regarding the training, validation and testing data used during the development of the system.
  o High data quality requirements for the development of AI high-risk systems, fully reflect guidance published by DPAs to ensure transparency, fairness, data minimisation, security.
  o DPAs are associated to regulatory sandboxes when AI systems process personal data. Where an AI application falls in their mandate, they shall have access to all documentation about that application and they can team up with market surveillance authorities to test AI systems.
BACKGROUND