Innspill fra Digdir til norsk posisjonsnotat:

EU-kommisjonens utkast til forordning for regulering av kunstig intelligens

Innledende kommentarer

Vi takker for muligheten til å gi innspill til en norsk posisjon til EU-kommisjonens forslag til en forordning for bruk av kunstig intelligens (COM (2021) 206 final).

Kunstig intelligens er et viktig område for Digdir. Bruk av kunstig intelligens kan gi store gevinster for samfunnet, næringsliv og innbyggere, men innebærer også risiko for misbruk og kan skade demokratiske prosesser og grunnleggende verdier og rettigheter. Regulering av kunstig intelligens kan vanskelig gjøres på en hensiktsmessig måte nasjonalt. Det er derfor nyttig at EU legger opp til en felles regulering i EUs indre marked.

Etter en første gjennomlesing ønsker vi å uttrykke støtte til forslaget, at det fremmes som en forordning og at hovedprinsippet er en risikobasert tilnærming. Intensjonen om å regulere i tråd med europeiske verdier, samtidig som reguleringen ikke blir så streng at den hemmer innovasjon, muligheter for europeiske konkurransekraft og effektivitet i offentlig sektor, er god. Vi vil likevel benytte anledningen til å komme med innspill til noen punkter, hvor det etter vårt syn for eksempel er behov for klargjøringer.

På nasjonalt nivå vil det fremover være viktig å kartlegge konsekvensene lovforslaget i sin nåværende form vil ha for norsk offentlig- og privat sektor generelt, og fra Digdirs perspektiv, for digitaliseringen av offentlig sektor spesielt.

Vi registrerer at noen av formuleringene i forslaget er relativt vage, for eksempel slår annex III, jamfør fortalepunkt 37 fast at essensielle offentlige løsninger som er «necessary for people to fully participate in society» skal regnes som "høy-risiko". Vi har forståelse for at formuleringene må være fleksible for at regelverket skal være fremtidsrettet og robust blant annet i møte med ny teknologi og nye bruksområder. En av erfaringene vi har gjort oss etter innføringen av GDPR er imidlertid at vage formuleringer, i kombinasjon med høye overtredelsesgebyrer, kan fremme en risikoavers kultur. Dette kan virke hemmende for innovasjon og utvikling. For norsk offentlig sektor, som nyter og er avhengig av høy tillitt i befolkningen, forsterkes risikoaversjonen av at overtredelsesgebyr kan medføre omdømmetap.

Digdir ser at forslagets art. 71 nr. 7 åpner for et nasjonalt handlingsrom om hvorvidt manglende etterlevelse skal kunne medføre overtredelsesgebyr for offentlig sektor. I lys av erfaringen over, oppfordrer vi departementet til å vurdere grundig om og hvordan vi kan ivareta innovasjonstakten og kulturen i offentlig sektor på en best mulig måte.

Forslaget vil medføre en del nye funksjoner og oppgaver som vil måtte legges til nye eller eksisterende offentlige virksomheter. Vi ser det som viktig at Norge må få en rolle i European Artificial Intelligence Board (EAIB), som foreslås opprettet i art. 56. Hvert medlemsland skal opprette National Competent Authorities (art. 59), hvorav en utnevnes til å være National Supervisory Authority og delta i EAIB. EAIB vil jobbe tett med EU-kommisjonen og skal bidra til å sikre harmonisert gjennomføring av forordningen. De vil også kunne gi uttalelser og retningslinjer.

Kommisjonen tillegges en del myndighet til å gi «forskrifter» i form av «delegated acts». I dette arbeidet skal Kommisjonen støttes av en komite (art. 74). Også i denne komiteen bør Norge tilstrebe å delta med en fagekspert. Dette vil også kreve ressurser.

Forslaget til forordning kan medføre store økonomiske og administrative konsekvenser for norsk offentlig sektor. Dette særlig fordi definisjonen av høy-risiko kunstig intelligens favner store oppgaver og fagområder for offentlig sektor, jf. annex III til forslaget. I den grad offentlig sektor vil være en «provider» av slik kunstig intelligens, vil offentlig sektor tillegges stort ansvar for kontroll, rapportering og øvrig etterlevelse av lovforslaget. Dette vil kreve økt ressurstilførsel, også før forordningen trer i kraft. Vi anser likevel at kostnadene som måtte følge av forslaget, er nødvendige og kan forsvares av nytten av reguleringen.

Digdir gjør oppmerksom på at i definisjonen i art. 3 nr. 1, (jamfør annex I bokstav c), omfattes statistisk metode av reguleringen, dersom den benyttes til å «*generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with».* Svært mye av offentlig forvaltnings arbeidsmetoder bygger på statistikk og statistiske metoder og vil antakeligvis falle inn under denne definisjonen. Dette gjelder f.eks. risikobaserte tilnærminger til kontroll og tilsyn osv. Digdir mener KMD bør se nærmere på hvordan definisjonen vil påvirke offentlig sektors handlingsrom og eventuelle økonomiske og administrative konsekvenser.

I tråd med artikkel 73 tillegges EU-kommisjonen myndighet til å gjøre endringer i både i annex I og annex III ved «delegated acts». Dette betyr at de kan endre definisjonene av kunstig intelligens og av høyrisiko kunstig intelligens. For Norge, som i mindre grad enn EUs medlemsland kan være en aktiv deltaker og påvirker i prosesser i EU-kommisjonen, kan dette bety at vi har liten mulighet til å påvirke hvordan omfanget av forordningen eventuelt kan utvikle seg.

Nedenfor følger våre foreløpige innspill til norsk posisjon til lovforslaget som kan videreformidles EU-kommisjonen. Forslaget som foreligger er svært omfattende, både med tanke på størrelse, men også at forslaget skal regulere et nytt felt. Det er derfor krevende å raskt vurdere konsekvensene av de foreslåtte reglene. Dette er foreløpige innspill etter begrenset tid til å sette oss inn i forslaget. Vi har skrevet innspillene nedenfor på engelsk, slik at de lettere kan tas med videre i et felles norsk posisjonsnotat.

1. EEA relevance

We notice that the draft regulation is not marked as EEA relevant. The Explanatory Memorandum point 2.1 lays down the TFEU art. 114 on the internal market as the legal basis for the proposal. We therefore proceed on the assumption that the regulation would be considered EEA relevant and will be adopted into the EEA agreement. We present our comments to the draft regulation in light of this, considering Norway as having to apply the regulation, possibly with some adjustments, as national law.

2. General remarks

The technological development in recent years has shown solutions using artificial intelligence systems to the benefit of society, businesses and citizens. But these technologies may also have a potential to cause harm on society and fundamental rights and values. We are in particular concerned about the risk that the use of artificial intelligence systems can pose to democratic processes and important fundamental values our societies are founded upon.

We support the Commission's position that the current European regulatory framework is insufficient to cover AI, and that soft law approaches such as ethical guidelines will not suffice. We, therefore,

strongly support the proposal to regulate the use of artificial intelligence systems to protect European values. We also support the proposed instrument of a regulation, to ensure consistency and a level playing field in the internal market. This is a necessary, ambitious and comprehensive proposal.

We appreciate the aim of balancing regulation with flexibility, and not imposing a higher than necessary burden on those providing or using artificial intelligence systems with limited risks. We recognise the challenge involved in striking the balance between innovation and regulation. The risk-based approach is a useful way to address this. However, there may be a risk that use of several low-risk AI systems together, may end up posing a higher risk. This is a point it may be necessary to consider in the future discussions on the proposal. There is currently little way of knowing what data-driven projects are being planned or, indeed, in production, which, as Brauneis and Goodman (2018) write, is a major transparency concern. That data-driven practices may have unintended societal consequences has been recognised but not problematised by most practitioners. This is due largely to the fact that their individual projects may indeed be innocuous and have minimal societal impact; when combined, however, "small" and fragmented initiatives may actually have a real impact on the state-citizen relationship. The majority of current projects are based on control. Each of these can be justified from an organisational perspective, but at a national level, the question needs to be asked of whether this is moving in the direction of better services to citizens, as envisioned, or could signify a shift towards more state control. (Broomfield & Reutter 2021).

We note that the main subjects of the regulation are the professional actors such as companies developing AI systems, or public sector authorities developing or using such systems. It seems citizens will have to go via the GDPR to safeguard their rights. We would consider it useful if – in the continued work on the proposed regulation – the interplay and demarcation between the two regulations be further clarified.

We consider it important to continue a coordinated approach and ensure a good level of harmonisation also with the work being done in the Council of Europe ad-hoc committee on artificial intelligence.

3. Risk-based approach

We note that the proposed regulation, to a larger extent than for instance the GDPR, take a risk-based approach to legal use of AI and obligations the various actors will have to comply with. We support this approach. To harvest the benefits artificial intelligence systems may bring to both the private and the public sector, we consider it to be a prerequisite that the regulation does not impose unnecessarily strict measures in situations where a low risk suggests that no specific measures should be necessary. We appreciate how the proposal reflects this.

4. European Artificial Intelligence Board

Given our assessment of EEA relevance of the proposed regulation, we would like to underline the importance for Norway of being included in the European Artificial Intelligence Board to be established in accordance with title VI, chapter I of the proposal. This will be essential to ensure consistent application of the regulation across the internal market.

5. Definition

According to the definition in art. 3 para. 1, ref. annex I letter c), statistical approaches are covered by the regulation in so far as they are used to "generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". We expect that

important parts of the activities of the public sector will fall under this definition, such as the use of statistical models. We ask that you be mindful that including statistical approaches leads to a very broad scope of the regulation and we suggest to thoroughly investigate the consequences of including “statistical approaches” in the definition of AI.

We note that according to art. 7, ref. art. 73, the Commission can make amendments to annex III. However, only within the scope of the areas already listed in annex III. In addition, the risks mentioned in art. 7, para 1 b) does not cover for instance a high risk of severe financial consequences or consequences for intellectual property rights. In this sense, annex III and the possibilities to amend it are rather narrow. To ensure a future proof regulation, it would be useful to discuss whether further amendments to annex III could be made in the future than what would be possible according to the current art. 7.

6. Wording – the need for harmonisation

We have noticed that the proposed regulation uses similar, but rarely identical, wording as in the GDPR. For instance, there are few references to the definitions given in the GDPR art. 4; the only definition that is similar for the two regulations is “biometric data”. Another example is the word “located”, which is used in the provision regulating the scope of the regulation (AIR art. 2 (b)), while the GDPR, when regulating the scope, uses the word “established”.

We would like to point out that we find it very important that the wording is harmonised when the meaning of a term in the two regulations is the same or close to similar. Such harmonisation is a precondition for possible future digitalization of the legislation itself or systems to follow up on compliance etc. Furthermore, unclear and vague wording may cause confusion amongst the users of the regulation. This can, in turn, not only complicate compliance process for users that must navigate both regulations but can also contribute to less harmonisation across the internal market. On this point, we would also respectfully like to make a reference to the work of the European Commission on “digital ready policies” that highlights the importance of using simple, precise and concise wording and to reuse existing concepts where possible.

7. Data and data governance (art. 10)

We find the requirements in art. 10, para. 3 strict. It will be hard, if not impossible, to ensure that data are fully “free of errors” and “complete”. Considering the high penalties for non-compliance with this article in particular, we would suggest softer wording on this point. Although data for training, validation and testing should be free of errors and complete to the extent possible, it cannot be an absolute requirement. We also consider data quality to be dependent on context: what may be sufficient data quality in one context, may not be good enough in another. Such differences in context can occur also within the scope of high-risk AI.

8. Transparency (art. 60 and 51)

We welcome the efforts to increase transparency by introducing an EU-wide database on high-risk stand-alone AI systems. However, the obligation for providers to register high-risk AI systems in the database, does not, in our view meet the demands for transparency on the use of AI by public authorities. It could therefore be considered if the efforts to increase transparency in this area, could be strengthened. The Regulation could impose a similar registration obligation for public authorities on all their use of AI systems, regardless of whether it is high or low risk.

9. Regulating deep-fakes and the exception for free speech

The Regulation in art. 51 imposes an obligation to disclose the use of deep-fakes. However, the proposed regulation stipulates that the obligation does not apply when the use of deep-fakes is necessary for the exercise of the right of free speech. While we appreciate the need to protect the right of free speech, we fear that this exception may in practice lead to the obligation to disclose the use of the techniques referred to in art. 51 having little practical effect.