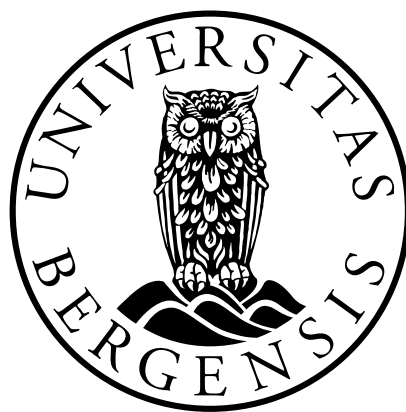


En rettslig analyse av hvorvidt GDPR gjelder for det parlamentariske arbeidet

Fullt ut, delvis eller ikke i det hele tatt?

Kandidatnummer: 41

Antall ord: 14624



JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. mai 2022

INNHOLDSFORTEGNELSE

INNHOLDSFORTEGNELSE	2
DEL I: INNLEDNING.....	5
1. PROBLEMSTILLING	5
2. PERSONVERNFORORDNINGEN (GDPR).....	5
2.1. Introduksjon til forordningen	5
2.2. Sprikende europeisk tilnærming.....	6
3. BAKTEPPEET FOR PROBLEMSTILLINGEN – DET PARLAMENTARISKE ARBEIDET	7
4. RETTSKILDER	8
4.1. Ordlyd og fortale	8
4.2. Rettsavgjørelser	9
4.3. Øvrige kilder	10
5. VIDERE BEHANDLING	11
5.1. Oppsummering av del I	11
5.2. Del II	11
5.3. Del III	11
5.4. Del IV	12
DEL II: GDPR SITT VIRKEOMRÅDE	13
1. SENTRALE DEFINISJONER	13
2. GDPR ARTIKKEL 2 NR. 2 BOKSTAV (A)	14
2.1. Om bestemmelsen	14
2.2. Ordlyd.....	15
2.3. Fortalepunkt (16) og rettspraksis fra EU-domstolen.....	16
2.3.1. Fortalepunkt (16).....	16
2.3.2. Rettspraksis	16
2.4. Det parlamentariske arbeidet og nasjonal sikkerhet.....	18
2.5. Østerrikes tilnærming	21
DEL III: UNNTAK FRA GDPR.....	23
1. ADGANGEN TIL Å GJØRE UNNTAK.....	23
1.1. Vernet om personopplysninger er ikke absolutt.....	23
1.2. Omfanget av begrensninger	23
1.3. Kravet til lovhjemmel.....	24
2. GDPR ARTIKKEL 85	26
2.1. Om bestemmelsen	26
2.2. Er «journalistic purposes and the purposes of academic, artistic or literary expression» en uttømmende angivelse av hva som kan begrunne unntak av hensyn til ytrings- og informasjonsfriheten?	27
2.2.1. Ordlyd.....	28
2.2.2. Betydningen av endringer fra direktiv 95/46/EC	29
2.2.3. Oppsummering	33

2.3.	Kan behandlingen av personopplysninger i det parlamentariske arbeidet unntas etter artikkel 85?	33
2.3.1.	Ordlyd.....	33
2.3.2.	Fortalepunkt (153).....	34
2.3.3.	Rettspraksis	34
2.3.4.	Danmarks tilnærming	38
3.	GDPR ARTIKKEL 23	39
3.1.	Om bestemmelsen	39
3.2.	De angitte formålene som kan hjemle en begrensning	40
3.3.	«[R]estriction».....	41
3.4.	«[R]espect the essence of the fundamental rights and freedoms»	43
3.4.1.	Ordlyd.....	43
3.4.2.	Rettspraksis	43
3.4.3.	EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR.....	44
3.5.	«[N]ecessary and proportionate measure in a democratic society to safeguard» de nærmere angitte formålene	45
4.	GDPR ARTIKKEL 23 OG DET PARLAMENTARISKE ARBEIDET	46
4.1.	Innledende	46
4.2.	Om det parlamentariske arbeidet.....	47
4.3.	Begrensning gjennom artikkel 23	48
4.4.	Hvor kan begrensningen hjemles?	51
	DEL IV: AVSLUTTENDE BEMERKNINGER	54
1.	PROBLEMSTILLINGER SOM BØR AVKLARES FØR EN EVENTUELL LOVENDRING.....	54
1.1.	«[C]ontroller» jf. artikkel 4 nr. 7	54
1.2.	«[S]upervisory authority» jf. artikkel 51 jf. artikkel 4 nr. 21	55
2.	BEHOV FOR AVKLARING PÅ EUROPEISK NIVÅ	58
3.	KONKLUSJON	59
	LITTERATURLISTE.....	60
	VEDLEGG.....	67

DEL I: INNLEDNING

1. Problemstilling

I denne masteroppgaven skal jeg vurdere hvorvidt Personvernforordningen (GDPR) gjelder for det parlamentariske arbeidet. Spørsmålet er om forordningen gjelder fullt ut, delvis eller ikke i det hele tatt for slikt arbeid.

2. Personvernforordningen (GDPR)

2.1. Introduksjon til forordningen

Gjennomføringen av Personvernforordningen (GDPR) inngår i Den europeiske union (EU) sitt mål om harmoniserte regelverk på tvers av Europa. Forordningen skal gi EU-borgere likt vern om personopplysninger. Myndigheten til å innføre et felleseuropeisk regelverk følger av Traktaten om Den europeiske unions virkemåte (TEUV) artikkel 16. Etter bestemmelsen skal Europaparlamentet og Rådet for Den europeiske unionen utforme «the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data [...]». På bakgrunn av dette har EU kompetanse til å pålegge regler – gjennom forordningen – ved behandling av personopplysninger.

I Norge er GDPR gjennomført ved lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven), som fastsetter at forordningen «gjelder som

norsk lov» med visse tilpasninger som følger av EØS-avtalen, jf. § 1.¹ Loven avløser den tidligere lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) som gjennomførte Europaparlamentets og Rådets direktiv 95/46/EC av 24. oktober 1995 om behandling av personopplysninger («95-direktivet»). Et direktiv gir rom for nasjonale variasjoner ved at myndighetene selv kan avgjøre hvordan direktivets bestemmelser skal gjennomføres i nasjonal rett. Til forskjell fra dette skal en forordning gjennomføres og grunnleggende sett tolkes og praktiseres likt – ord for ord – i alle medlemsland.² Tanken er at lik standard på regelverket styrker personvernet til EU-borgerne. Vedtakelsen av en forordning fremfor et direktiv er derfor et utslag av EUs mål om et harmonisert lovverk i Europa.

Oppgaven gjengir utdrag fra forordningen, fortalen og EU-domstolens avgjørelser på engelsk. Til forskjell fra norsk utgjør engelsk en autoritativ språkversjon. Der det er behov for å forklare begreper nærmere, vil forklaringen gis fortløpende og ikke i et eget kapittel.

2.2. Sprikende europeisk tilnærming

Formålet om å gi de registrerte³ et omfattende vern gjør at GDPR er utformet både abstrakt og generelt. Samtidig medfører generelle og abstrakte formuleringer et større tolkningsrom, som igjen kompliserer formålet om en unison forståelse på tvers av medlemslandene. Spørsmålet om i hvilken grad GDPR gjelder for det parlamentariske arbeidet er et eksempel på at medlemslandene tolker forordningen forskjellig.

En rapport innhentet av parlamentet i Østerrike illustrerer en sprikende europeisk tilnærming til spørsmålet om forordningen gjelder for det parlamentariske arbeidet eller ikke.⁴

¹ Se EØS-avtalen vedlegg XI nr. 5e. Tilpasningene innebærer blant annet at en rekke av henvisningene i forordningen – eksempelvis «Member State» og «supervisory authority» – også inkluderer EFTA-landene og dermed Norge. Det er ikke av betydning for oppgaven å adressere dette nærmere.

² SE TEUV artikkel 288; Fredriksen og Mathisen, *EØS-rett* (2018) s. 363; Schartum, *Personvernforordningen* (2020) s. 17

³ Betegnelsen brukes om dem hvis rettigheter forordningen skal ivareta, jf. artikkel 2 nr. 1 jf. artikkel 4 nr. 1. Forordningens virkeområde behandles inngående i del II.

⁴ ECPRD, *REQUEST 4673* (2021)

Majoriteten av medlemslandene anser GDPR for å regulere spørsmålet. En andel av disse mener likevel at unntak må kunne gjøres for deler av det parlamentariske arbeidet. Enkelte land anser derimot det parlamentariske arbeidet som utenfor forordningens virkeområde. Norge har ikke oppgitt sitt standpunkt i rapporten. I denne oppgaven søker jeg å se på hvordan Norge bør vurdere dette spørsmålet.

Den videre drøftelsen under punkt 3 skisserer det parlamentariske arbeidet for å sette problemstillingen i kontekst.

3. Bakteppet for problemstillingen – det parlamentariske arbeidet

Opgaven skal vurdere bruken av GDPR der personopplysninger behandles i stortingsrepresentantenes parlamentariske arbeid. Spørsmålet er prinsipielt og må avklares før en kan ta stilling til om forordningens øvrige vilkår – for eksempel om krav til behandlingsgrunnlag – er innfridd. Disse vurderingene forutsetter at forordningen kommer til anvendelse.

Begrepet «parlamentarisk arbeid» omfatter de arbeidsoppgavene som inngår i en stortingsrepresentants virke som folkevalgt. Det parlamentariske arbeidet skal ivareta ulike funksjoner. De mest sentrale er å fatte beslutninger og vedtak i salen, som for eksempel lover, (beslutningsfunksjon), behandle ulike budsjettsaker (bevilgende funksjon) og gjennomføre spørretimer, interpellasjoner og arbeid i Riksrevisjonen og EOS-utvalget (kontrollfunksjon).⁵ For arbeid knyttet til beslutnings- og bevilgningsfunksjonen, foregår mye av det parlamentariske arbeidet innen fagkomiteene som de respektive stortingsrepresentantene er del av. Arbeid med partigruppene og deltakelse i debatter og voteringer utgjør også en sentral

⁵ Se Grunnloven § 75 flg.; Smith (2017) *Konstitusjonelt demokrati*, s. 196

del av det parlamentariske arbeidet.⁶ Denne oppgaven vil ta utgangspunkt i det parlamentariske arbeidet som angitt her, men også aktiviteter som e-postutveksling og annen møtevirksomhet som utføres i virket som stortingsrepresentanter er omfattet.

Det parlamentariske arbeidet er en forutsetning for demokratiets funksjon, og karakteristikkene ved arbeidet er særpreget av stortingsrepresentantenes rolle som folkevalgte. Uavhengigheten som følger med å være folkevalgt gjør at Stortingets administrasjon ikke har styringsrett overfor representantene – de er «ansatt av folket». Stortingsrepresentantenes plikter er forankret og delvis regulert i Grunnloven, herunder i Grl. § 63 flg.

4. Rettskilder

4.1. Ordlyd og fortale

Drøftelsen av problemstillingen bygger på europeisk rettskildelære. Ordlyden i forordningens bestemmelser veier særlig tungt som følge av EUs ønske om færrest mulig nasjonale variasjoner.

Som nevnt innledningsvis, er bestemmelsene i GDPR ofte utformet generelt og abstrakt for å gi vern på et bredt spekter av områder. De vide formuleringene kan i mange tilfeller gjøre det vanskelig å trekke konkrete slutninger basert på forordningens ordlyd alene. Av denne grunn er forordningens fortale også et viktig tolkningsbidrag som kan brukes «so far as they set out the reasons for its adaptation [...] or [...] illustrate the object and purpose of a legislative act» jf. de generelle uttalelsene i avsnitt 45 i *Nilsson and others [C5]*, C-162/97. EU-domstolen presiserte samtidig at fortalen «have no binding legal force of themselves and independently

⁶ *Stortinget*, «Hva gjør en representant?»

of the operative provisions of that act». Dermed kan fortalen brukes for å utfylle og forklare hva som er innholdet i de enkelte bestemmelsene, men den har likevel isolert sett ikke selvstendig rettskildemessig verdi.

4.2. Rettsavgjørelser

Rettsavgjørelser fra EU-domstolen er viktige rettskilder i tolkningen av GDPR. Domstolens uttalelser avklarer hvordan forordningen skal forstås. Graden av rettsavgjørelsens presedens må blant annet vurderes ut fra hvor generell eller spesifikk uttalelsene til domstolen er, og i hvilken grad rettsspørsmålet i dommen ligner på rettsspørsmålet som er gjenstand for tolkning.

Omfanget av rettspraksis som angår tolkningen av GDPR er begrenset ettersom forordningen er relativt ny (2018). GDPR er imidlertid en videreføring av 95-direktivet, og rettstilstanden under direktivet kan få betydning for forståelsen av forordningens bestemmelser.

Forordningen har en rekke bestemmelser som er ment som en videreføring av direktivet. Likevel kan variasjoner i både utforming og innhold forekomme, og det må følgelig adresseres hvorvidt den etablerte tolkningen av en bestemmelse i direktivet gir bidrag til forståelsen av forordningen. Relevansen av rettstilstanden etter direktivet må avklares ut fra en sammenligning av de to bestemmelsene. Ved nyanser eller ulikheter bør betydningen av dette vurderes før direktivet brukes som tolkningsbidrag.⁷

Ettersom GDPR er vedtatt på overnasjonalt nivå, har tolkningen og praktiseringen i de ulike medlemslandene liten autoritativ betydning. I mangel på formelle rettskilder kan nasjonale tolkninger likevel ha vekt, først og fremst fra nasjonale domstoler. Der dette ikke foreligger kan også relevante saker fra datatilsyn og klagemyndigheter tjene som illustrasjon. Kildene

⁷ Schartum, *Personvernforordningen*, (2020) s. 25

viser hvordan GDPR blir håndhevet i praksis, men tolkningen er likevel ikke rettslig bindende.

4.3. Øvrige kilder

I 2021 gjennomførte parlamentet i Østerrike en undersøkelse der spørsmålet om GDPR sin anvendelse på det parlamentariske arbeidet ble rettet mot de øvrige parlamentene i EU/EØS for å kartlegge deres tolkning av forordningen. Funnene fra denne undersøkelsen ble oppsummert i rapporten «ECPRD-REQUEST 4673 concerning the GDPR'S APPLICATION IN PARLIAMENTARY CORE AREAS FINAL SUMMARY» som er publisert i The European Centre for Parliamentary Research and Documentation (ECPRD). Rapporten har ingen selvstendig verdi som rettskilde, men den gir likevel innblikk i hvordan øvrige parlamenter i EU/EØS har vurdert GDPR sitt anvendelsesområde på det parlamentariske arbeidet.

På bakgrunn av rapporten har jeg korrespondert med utvalgte parlamenter i Europa. Enkelte drøftelser i denne oppgaven vil vise til innhold fra korrespondansene.⁸ Bruken søker utelukkende å belyse hvordan ulike parlamenter i Europa begrunner sin tolkning av den samme problemstillingen som denne oppgaven angår, og vil i hovedsak kommenteres der disse avviker fra mine tolkninger eller der de brukes til inspirasjon for egne innfallsvinkler. Enkelte drøftelser viser også til møtereferat som forklarer de praktiske konstellasjonene på Stortinget. Ingen av de nevnte kildene har rettskildemessig vekt.

Fremstillingen er oppdatert per 05.05.2022.

⁸ I hovedsak publiserte artikler og utredninger fra de respektive landene.

5. Videre behandling

5.1. Oppsummering av del I

Gjennomgangen i punkt 3 viser sentrale aspekter ved det parlamentariske arbeidet. Spørsmålet om dette arbeidet er underlagt GDPR må bygge på europeisk rettskildelære, skissert i punkt 4.

Selv om fremstillingen begrenses til stortingsrepresentantenes parlamentariske arbeid, er problemstillingen også relevant for andre institusjoner. I likhet med Stortinget vil eksempelvis regjeringen ha lignende problemstillinger overfor statsråder, som også er ombudsmenn. Politikere i kommuner og fylkeskommuner vil kunne oppleve tilsvarende utfordringer.

5.2. Del II

I del 2 tar jeg stilling til forordningens virkeområde ved å vurdere om GDPR i det hele tatt regulerer det parlamentariske arbeidet på bakgrunn av artikkel 2 nr. 2. Bestemmelsen avgrensner forordningen sitt virkeområde. Rettskildene tyder på at det parlamentariske arbeidet inngår i det forordningen regulerer.

5.3. Del III

Gitt at forordningen regulerer behandling av personopplysninger i det parlamentariske arbeidet, vurderer jeg i del 3 anvendelsen av eventuelle unntak. Punkt 1 gir en overordnet begrunnelse for adgangen til å gjøre unntak.

Punkt 2 behandler unntaksbestemmelsen i artikkel 85. På bakgrunn av analysen mener jeg bestemmelsen ikke åpner for unntak for det parlamentariske arbeidet.

Punkt 3 drøfter vilkårene for begrensning etter artikkel 23. Bestemmelsen åpner etter mitt syn potensielt for å at forordningens anvendelse på deler av det parlamentariske arbeidet kan begrenses. Gjennomgangen skisserer derfor også hvorfor og hvordan artikkel 23 kan være en aktuell begrensningshjemmel av hensyn til det parlamentariske arbeidet.

5.4. Del IV

I del IV gir jeg bemerkninger til en eventuell begrensningshjemmel for det parlamentariske arbeidet i norsk rett, og adresserer behovet for rettsavklaring på både nasjonalt og overnasjonalt nivå.

DEL II: GDPR SITT VIRKEOMRÅDE

1. Sentrale definisjoner

Personvernforordningens saklige virkeområde omfatter helt eller delvis automatisert «processing of personal data» og ikke-automatisert behandling som inngår i eller skal inngå i et register, jf. artikkel 2 nr. 1. Med «processing» regnes «any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means». Som eksempler nevnes blant annet innsamling, registrering, lagring, gjenfinning og sletting. Vilkåret omfatter derfor all informasjon som enten kan knyttes til en spesifikk person eller bidra til å identifisere en fysisk person, og som prosesseres av noen andre enn personen selv, jf. artikkel 4 nr. 2.

Vilkåret «personal data» er definert i artikkel 4 nr. 1. Definisjonen er vid og omfatter «any information relating to an identified or identifiable natural person ('data subject')». En «identifiable natural person» er videre definert som «one who can be identified, directly or indirectly» særlig gjennom en «identifier» – eksempelvis ved navn og lokaliseringsopplysninger. Opplysninger som kan sammenstilles til å identifisere en fysisk person er dermed også å regne som «personal data». Det følger av definisjonen at virkeområdet til forordningen er vidtrekkende.

Et vidtrekkende virkeområde samsvarer med fortalepunkt (10) som uttrykker et ønske om å «ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union» og at «the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States». Formålet kan overordnet ses i lys av prinsippet om de fire friheter – fri flyt av varer, tjenester, kapital og personer over landegrensene og fravær av diskriminering på bakgrunn av nasjonalitet. Prinsippet innebærer at nasjonale lover og regler

ikke skal være til hinder for muligheten for fri bevegelse. EU-borgere skal blant annet ha de samme rettighetene som statsborgerne i det EU-landet de bosetter seg i, så lenge dette er innenfor traktatens virkeområde.⁹ I dette ligger også at alle skal ha samme vern om sine personopplysninger innen samme virkeområde.

I GDPR artikkel 2 nr. 2 gjøres det visse begrensninger i forordningens virkeområde. Det parlamentariske arbeidet er ikke uttrykkelig omtalt i denne forbindelse, hverken i artikkel 2 nr. 2 eller i fortalen. Motsetningsvis er for eksempel domstolenes virksomhet uttrykkelig omtalt i fortalepunkt (20). Ved behandling av personopplysninger i den dømmende virksomheten – som når de treffer avgjørelser – er domstolene unntatt tilsynsmyndighetenes kompetanse.¹⁰ Ettersom det parlamentariske arbeidet ikke uttrykkelig er unntatt forordningens virkeområde, må utgangspunktet være at GDPR gjelder for dette arbeidet.

Den videre drøftelsen vil i punkt 2 gå i dybden av forordningens virkeområde. Hensikten er å undersøke om det parlamentariske arbeidet på tross av utgangspunktet likevel må sies å falle utenfor det forordningen er ment å regulere. Drøftelsen vurderer om det parlamentariske arbeidet omfattes av vilkåret «outside the scope of Union law» i artikkel 2 nr. 2 bokstav (a).

2. GDPR artikkel 2 nr. 2 bokstav (a)

2.1. Om bestemmelsen

Artikkel 2 nr. 2 avgrensner forordningens virkeområde. Bokstavene (a) til (d) angir tilfeller der behandling av personopplysninger ikke omfattes av forordningen. Etter bokstav (a) skal forordningen ikke gjelde behandling av personopplysninger «in the course of an activity

⁹ Trondal (2019)

¹⁰ Se også GDPR artikkel 55 nr. 3. Begrunnelsen er å «safeguard the independence of the judiciary in the performance of its judicial tasks» jf. fortalepunkt (20).

which falls outside the scope of Union law¹¹». Dersom det parlamentariske arbeidet skal tolkes som utenfor forordningens virkeområde, er det dette alternativet som er det mest aktuelle å vurdere.

Forordningen bruker i artikkel 2 begrepet «activity» for å *avgrense* mot områder som ikke reguleres av GDPR. Tilsvarende er betegnelsen «activity» brukt i artikkel 85 for å regulere adgangen til å *unnta* områder som i utgangspunktet er regulert av GDPR fra forordningens bestemmelser. Artikkel 23 bruker ikke betegnelsen «activity» slik som artikkel 2 og 85, men åpner i stedet opp for at det kan gjøres *begrensninger* i nærmere angitte forpliktelser og rettigheter som følger av forordningen. Denne språklige forskjellen tolker jeg som at en «activity» vil avgrenses eller unntas i sin helhet etter artikkel 2 og 85. En anvendelse av artikkel 23 vil derimot ikke nødvendigvis innebære en begrensning av forpliktelser og rettigheter innenfor en «activity» i sin helhet. Det er, slik jeg leser bestemmelsen, etter artikkel 23 heller et spørsmål om det kan gjøres begrensninger i *enkelte deler* av en «activity» dersom bestemmelsen øvrige vilkår er innfridd. Vurderingen av artikkel 2 innebærer dermed, slik jeg forstår bestemmelsene, at det vil være et spørsmål om det finnes rettskildemessige holdepunkter for å si at det parlamentariske arbeidet *i sin helhet* er en «activity» som faller «outside the scope of Union law» og slik også utenfor GDPR sitt virkeområde jf. artikkel 2 nr. 2 bokstav (a).

2.2. Ordlyd

Ordlyden «activity which falls outside the scope of Union law» tilsier en avgrensning mot områder som ligger utenfor EUs mandat å regulere. Ordlyden gir ikke anvisning på relevante momenter for en slik vurdering. Men gjennom fortalepunkt (16) og rettspraksis fra EU-domstolen er det likevel gitt føringer på forståelsen av «outside the scope of Union law».

¹¹ Etter EØS-avtalen vedlegg XI nr. 5e omfatter «Union law» EØS-avtalen og bestemmelsene om vern av personopplysninger i EØS-avtalen, med mindre annet er bestemt.

2.3. Fortalepunkt (16) og rettspraksis fra EU-domstolen

2.3.1. Fortalepunkt (16)

Hva som menes med «outside the scope of Union law» er ikke utførlig behandlet i fortalen. Likevel står det i fortalepunkt (16) at forordningen ikke får anvendelse for behandling av personopplysninger «concerning national security». Fortalepunkt (16) nevner også EUs felles utenriks- og sikkerhetspolitikk som utenfor forordningens virkeområde, og dette er uttrykkelig unntatt forordningen etter artikkel 2 nr. 2 bokstav (b).

2.3.2. Rettspraksis

EU-domstolens rettsavgjørelse *Land Hessen* [C3], C-272/19, omhandler hovedsakelig spørsmålet om begjæringsutvalget i Land Hessen-parlamentet kan anses som «controller», altså behandlingsansvarlig, etter GDPR artikkel 4 nr. 7. Domstolen konkluderer med at begjæringsutvalget, som er en del av den tyske parlamentariske institusjonen, er å anse som «controller».

EU-domstolen vurderte imidlertid også om forordningen i det hele tatt kom til anvendelse for begjæringsutvalgets arbeid, og uttalte i den forbindelse at «since Article 2(2)(a) [...] constitutes an exception to the very wide definition of the scope of that regulation set out in Article 2(1) [...], Article 2(2)(a) must be interpreted restrictively» jf. avsnitt 68. Hva som menes med en restriktiv tolkning er nærmere presisert i EU-domstolens avgjørelse *Latvijas Republikas Saeima* [GC], C-439/19 avsnitt 62. Dommen omhandler offentliggjøring av personopplysninger ved veitrafikklovbrudd. Et avgjørende spørsmål for domstolen var om

behandling av personopplysninger i forbindelse med lovregulering av veitrafikk var «outside the scope of Union law» i GDPR artikkel 2 nr. 2 bokstav (a).

Når det gjelder en restriktiv fortolkning av artikkel 2 nr. 2 bokstav (a), uttalte domstolen at «Article 2(2)(a) of the GDPR is to be read in conjunction with Article 2(2)(b) thereof and recital 16», jf. avsnittene 62 og 63. Domstolen uttalte videre at den restriktive tolkningen medfører at bestemmelsen er «designed solely to exclude from the scope of that regulation the processing of personal data carried out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category» jf. avsnitt 66. Følgelig skal arbeid definert som nasjonal sikkerhet i utgangspunktet anses å falle utenfor forordningen. Som bakgrunn for konklusjonen påpeker domstolen i avsnitt 64 at forordningen viderefører bestemmelsen i direktiv 95/46/EC artikkel 3 nr. 2, og at forordningens bestemmelse derfor ikke kan tolkes «in broader terms» enn det som fulgte av direktivet. Tilsvarende er uttalt av EU-domstolen i *Land Hessen* avsnitt 67, der det fremgår at GDPR artikkel 2 nr. 2 «corresponds, in essence» med direktivet artikkel 3 nr. 2.

Uttalelsene over tolkes som at det parlamentariske arbeidet i sin helhet må vurderes som «processing of personal data carried out by State authorities in the course of an activity which is intended to safeguard national security» for å falle utenfor forordningens virkeområde etter artikkel 2 nr. 2 bokstav (a). For å avgjøre om hele det parlamentariske arbeidet kan unntas etter artikkel 2 nr. 2 bokstav (a), må innholdet av nasjonal sikkerhet derfor avklares.

I *Latvijas Republikas Saeima* konkluderte EU-domstolen med at «activities relating to road safety do not pursue» nasjonal sikkerhet som artikkel 2 nr. 2 bokstav (a) tar sikte på. Domstolen uttalte at nasjonal sikkerhet etter artikkel 2 nr. 2 bokstav (a) jf. fortalepunkt (16) omfatter «in particular, as the Advocate General has also observed [...] those [activities] that are intended to protect essential State functions and the fundamental interests of society» jf. avsnitt 67. I de refererte uttalelsene skriver generaladvokaten – med henvisning til øvrig EU-lovgivning – at nasjonal sikkerhet «is in this context to be understood as ‘State security’». I tillegg fremholdt generaladvokaten at artikkel 2 nr. 2 bokstav (a) bør leses i lys av TEU

artikkel 4 nr. 2 som nedfeller at EU må «respect Member States' essential State functions». Bestemmelsen gir som eksempel at «national security remains the sole responsibility of each Member State». EU-domstolens konklusjon gir generelle uttalelser som gjør at avgjørelsen har betydning ut over den konkrete saken, og den er dermed av betydning for forståelsen av nasjonal sikkerhet.

2.4. Det parlamentariske arbeidet og nasjonal sikkerhet

En forutsetning for å anse det parlamentariske arbeidet som «outside the scope of Union law» er følgelig at det kan sies å være «intended to protect essential State functions and the fundamental interests of society» jf. *Latvijas Republikas Saeima* avsnitt 67. Denne avgrensningen samsvarer med Traktaten om Den europeiske union (TEU)¹² artikkel 4, der det heter i nr. 1 at «competences not conferred upon the Union in the Treaties remain with the Member States». Som nærmere beskrevet i TEU artikkel 4 nr. 2, innebærer dette blant annet at EU skal respektere medlemsstatenes «essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State». *Rekkevidden* av nasjonal sikkerhet og hvordan begrepet nærmere skal defineres, gir imidlertid hverken forordningen, TEU artikkel 4 eller praksis fra EU-domstolen veiledning på. Heller ikke i fortalen til forordningen er rekkevidden eller innholdet behandlet.

Som oppgavens innledning har vist, var formålet med overgangen fra direktiv til forordning at man ønsket en felles forståelse og overholdelse av det europeiske regelverket. Konsekvensen av at nasjonal sikkerhet ikke er gitt en innholdsmessig avgrensning gjennom EU-retten, kan være at medlemsstatene selv definerer en videre forståelse av begrepet enn det lovgiver har ment som «activity which falls outside the scope of Union law». De potensielle nasjonale variasjonene vil således kunne stride mot EU-retten og dens prinsipper som ofte er ment å ha et autonomt innhold. Samtidig illustrerer TEU artikkel 4 at det finnes skranker for hvor langt

¹² Som sammen med TEUV inngår i primærretten og regulerer det grunnleggende forholdet mellom EU og medlemslandene.

EU-retten kan gå i sine rettslige reguleringer, særlig med hensyn til medlemsstatenes nasjonale suverenitet. Suverenitetsbetraktninger kan tilsi at EU-domstolen vil være varsom med å konkretisere rekkevidden av hva som inngår i nasjonal sikkerhet. Likevel kunne en veiledning fra for eksempel EU-domstolen med relevante momenter være hensiktsmessig for å unngå at artikkel 2 nr. 2 (a) blir en sekkebestemmelse som avgrenser GDPR sitt virkeområde gjennom vide nasjonale definisjoner av nasjonal sikkerhet.

Betydningen av nasjonal sikkerhet har en naturlig side mot nasjonal suverenitet, og statene vil kunne ha ulike oppfatninger av hva som ligger i begrepet. Som eksempel gir lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven) anvisninger på hva som i Norge er ment som «nasjonal sikkerhetsinteresse» i § 1-5. Selv om den norske loven ikke gir tolkningsbidrag til forståelsen av GDPR, illustrerer den hva lovgiver i Norge har vektlagt. Formålet med sikkerhetsloven er definert i § 1 og angir at loven skal ivareta Norges nasjonale sikkerhetsinteresser som § 1-5 nr. 1 bokstav (a) til (d) definerer som «landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til (a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet, (b) forsvar, sikkerhet og beredskap, (c) forholdet til andre stater og internasjonale organisasjoner, (d) økonomisk stabilitet og handlefrihet og (e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet».

Hva som er ment å omfattes av definisjonen i sikkerhetsloven § 1-5 nr. 1 bokstav (a) til (e) er i noen grad presisert i forarbeidene.¹³ Det fremgår her at sikkerhetstiltak som iverksettes for å ivareta «nasjonale sikkerhetsinteresser» må gjennomføres på en måte som samsvarer med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.¹⁴ Med grunnleggende rettsprinsipper og verdier sikter forarbeidene blant annet til hensynet til den enkeltes personvern og rettssikkerhet. Det uttales at det i dette «ligger en presisering av at det kun er de sikkerhetsmessige tiltakene som er nødvendig og forholdsmessig, og har en dokumentert effekt som skal iverksettes. Det ligger også en plikt til å vurdere alternative og mindre inngripende tilnærminger for å oppnå samme effekt».¹⁵ Ut over dette gir ikke forarbeidene

¹³ Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet

¹⁴ Prop. 153 L (2016-2017), s. 164

¹⁵ *Ibid.*

føringer på hva den innholdsmessige forståelsen av «nasjonale sikkerhetsinteresser» er. Henvisningen til at det må gjøres en forholdsmessig vurdering mellom behovet for sikkerhetstiltak og blant annet personvern og rettssikkerheter, taler likevel for at hva som er å anse som nasjonal sikkerhetsinteresse må vurderes konkret.

Som gjennomgangen her viser, gir hverken EU-retten eller nasjonal lovgivning i Norge klare avgrensninger på den innholdsmessige forståelsen av nasjonal sikkerhet. Det er likevel nærliggende å tenke at deler av det parlamentariske arbeidet ivaretar nasjonale sikkerhetsinteresser, både etter EU-retten og nasjonal forståelse. Dette vil for eksempel kunne gjelde arbeid knyttet til utenriks- og forsvarskomiteen og kontroll- og konstitusjonskomiteen, da disse ofte behandler saker som angår territoriell beskyttelse, grunnlovsmessige problemstillinger og forsvarsmessige hemmeligheter. Da det parlamentariske arbeidet samtidig kan være knyttet til arbeid som helse, natur og velferdsgoder, er det likevel tvilsomt at *hele* det parlamentariske arbeidet kan sies å utgjøre en nasjonal sikkerhet.¹⁶ Det kan også nevnes – dog uten rettskildemessig betydning – at Norges sikkerhetsmyndighet (NSM) i sin definisjon av «nasjonale sikkerhetsinteresser» uttaler at «deler av» Stortingets arbeid er omfattet av begrepet.¹⁷

GDPR sitt virkeområde etter artikkel 2 nr. 2 bokstav (a) tolkes som en avgrensning mot «activity» som i sin helhet faller «outside the scope of Union law». Da det etter denne gjennomgangen ikke er holdepunkter for å legge til grunn at det parlamentariske arbeidet i sin helhet er «intended to protect essential State functions and the fundamental interests of society» jf. *Latvijas Republikas Saeima* avsnitt 67, og dermed heller ikke «outside the scope of Union law» jf. GDPR artikkel 2 nr. 2 bokstav (a), er det her ikke avgjørende å gå nærmere inn på betydningen av EU-rettens manglende føringer på nasjonal sikkerhet.

Grensedragningen mellom skranken for EUs lovgivningsmyndighet og nasjonal suverenitet – og dermed blant annet medlemsstatenes egne definisjoner av nasjonal sikkerhet – vil følgelig heller ikke behandles mer inngående. Utgangspunktet er derfor at forordningen kommer til

¹⁶ Se Referat, Stortingets sikkerhetsstab (2022); Nærmere drøftelse av komitéarbeid og nasjonal sikkerhet følger av drøftelsen i del 3 punkt 4.2. og 4.3 om artikkel 23

¹⁷ Nasjonal sikkerhetsmyndighet, Figur 3.2.

anvendelse for det parlamentariske arbeidet. Videre må det vurderes om det er bestemmelser i GDPR som regulerer adgangen til å unnta hele eller deler av det parlamentariske arbeidet.

2.5. Østerrikes tilnærming

Østerrike tolker GDPR sitt virkeområde etter artikkel 2 nr. 2 bokstav (a) som en avgrensning mot det parlamentariske arbeidet. Mer konkret mener de at det parlamentariske arbeidet er en «activity which falls outside the scope of Union law» jf. artikkel 2 nr. 2 bokstav (a).¹⁸ Dermed er det deres nasjonale databeskyttelseslovgivning som regulerer de registrertes rettigheter, og denne gjelder også for det parlamentariske arbeidet.

Østerrike reiser spørsmål ved uttalelsene i *Land Hessen* om at «outside the scope of Union law» i GDPR artikkel 2 nr. 2 bokstav (a) ikke kan tolkes videre enn 95-direktivet artikkel 3 nr. 2. Argumentasjonen deres bygger særlig på at ordlyden i de respektive bestemmelsene er forskjellige.¹⁹ De viser til at direktivet artikkel 3 nr. 2 anga spesifikke aktiviteter som falt utenfor vilkåret om unionsrettens område, og at betydningen av en restriktiv tolkning derfor er annerledes enn for forordningen som ikke angir aktuelle aktiviteter.

Likevel er det ikke bestridt at GDPR artikkel 2 nr. 2 bokstav (a) og «outside the scope of the Union law» bygger på direktivet artikkel 3 nr. 2 – inkludert områdene som der er angitt, jf. blant annet *Latvijas Republikas Saeima* avsnitt 64 og 65.

Østerrike argumenterer videre for at rettspraksis knyttet til tolkningen av GDPR artikkel 2 nr. 2 mangler prejudikatsverdi, som følge av at de mener *Land Hessen* gjelder et spesielt tilfelle.²⁰ Som vist over, gir imidlertid EU-domstolen i *Land Hessen* generelle og prinsipielle

¹⁸ König (2022); Posnik (2021)

¹⁹ Posnik (2021) s. 157—158

²⁰ Posnik, (2021) s. 159; *Summary of the Request for a Preliminary Ruling*, C-33/22, s. 5 punkt 15. Den endelige avgjørelsen fra EU-domstolen er ikke offentliggjort enda.

uttalelser om hvordan de respektive bestemmelsene skal forstås. Disse uttalelsene har prejudikatsverdi, og omfatter blant annet konstateringen av at GDPR artikkel 2 nr. 2 bokstav (a) skal tolkes restriktivt. Prejudikatsverdien styrkes av at uttalelsene er fulgt opp og presisert i senere rettspraksis, herunder i *Latvijas Republikas Saeima*, se avsnitt 63. Hertil angikk *Land Hessen* behandling av personopplysninger i en begjæringskomité under det parlamentariske arbeidet, og denne parallellen kan gi saksforholdet i dommen ytterligere relevans for problemstillingen i denne oppgaven.

Østerrike argumenterer også for at begrensningene i tilsynskompetansen overfor domstolers behandlingsaktiviteter etter GDPR artikkel 55 nr. 3 har betydning for spørsmålet om forordningen og det parlamentariske arbeidet. Bestemmelsen fastslår at forordningen ikke gjelder når en domstol behandler personopplysninger i den dømmende virksomheten, altså i forbindelse med enkeltsaker. Østerrike fremhever at tilsyn med parlamentariske aktiviteter ikke vil være mindre problematisk enn slik kontroll av rettsvesenet.²¹ De mener dette underbygger en forutsetning om at det parlamentariske arbeidet var ment unntatt forordningen.²² Håndhevelsen av tilsyn overfor det parlamentariske arbeidet vil riktignok reise utfordringer i praksis.²³ De praktiske utfordringene er imidlertid ikke et rettslig argument som gir bidrag til tolkningsspørsmålet.

Videre kan den manglende unntakelsen av tilsyn med det parlamentariske arbeidet også være et argument for arbeidet nettopp *skal* omfattes av GDPR. At lovgiverne fant grunn til å eksplisitt unnta rettssystemet fra tilsyn, men ikke det parlamentariske arbeidet, må heller tolkes som en forutsetning for at slikt arbeid er underlagt forordningen. Dette samsvarer best med utgangspunktet om at det er eventuelle unntak fra forordningen som må begrunnes. I lys av dette styrkes behovet for en klar unntakshjemmel ytterligere av at en ekskludering fra GDPR sitt virkeområde vil omfatte *hele* det parlamentariske arbeidet som «activity».

²¹ König (2022) s. 5; Posnik (2021) s. 158—159

²² Se *Summary of the Request for a Preliminary Ruling*, C-33/22, s. 5 punkt 17.

²³ Utfordringer knyttet til håndhevelsen av tilsyn for det parlamentariske arbeidet adresseres avslutningsvis i del IV pkt. 1.2.

DEL III: UNNTAK FRA GDPR

1. Adgangen til å gjøre unntak

1.1. Vernet om personopplysninger er ikke absolutt

Forutsatt at det parlamentariske arbeidet faller inn under GDPR sitt virkeområde etter artikkel 2, må det vurderes om det kan gjøres *unntak fra* eller *begrensninger i* forordningen for det parlamentariske arbeidet.

Adgangen til å gjøre unntak fra eller begrense forordningen er en konsekvens av at vernet om de registrertes personopplysninger ikke er en absolutt rettighet. Illustrerende uttaler fortalepunkt (4) om GDPR artikkel 1 nr. 2 at «[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality [...]». Vernet om personopplysninger kan altså i enkelte tilfeller innskrenkes av hensyn til andre grunnleggende rettigheter.

1.2. Omfanget av begrensninger

Bestemmelsene i artikkel 23 og artikkel 85 åpner for henholdsvis begrensning av og unntak fra rettighetene og pliktene etter GDPR for å balansere andre grunnleggende rettigheter.

Unntaksadgangen er i utgangspunktet mest omfattende etter artikkel 85. Denne bestemmelsen fastsetter at medlemsstaten «shall provide for exemptions or derogations» fra potensielt syv kapitler i forordningen dersom dette er «necessary» for å avveie ytrings- og informasjonsfriheten av hensyn til de opplistede formålene, mot vernet om personopplysninger.

Artikkel 23 åpner på sin side for at medlemslandene kan «restrict [...] the scope of the obligations and rights» nedfelt i den konkrete bestemmelsen, dersom øvrige vilkår er innfridd. Bruken av «restrict» åpner for begrensninger og dermed ikke unntak som etter artikkel 85.

Virkingen av de respektive bestemmelsene har altså ulikt omfang. Begge bestemmelsene krever imidlertid at begrensningen eller unntaket er hjemlet i lov, og den videre drøftelsen vil først behandle vilkåret om lovhjemmel samlet i punkt 1.3. Deretter følger en gjennomgang av unntaksadgangen for det parlamentariske arbeidet etter henholdsvis artikkel 85 (punkt 2) og artikkel 23 (punkt 3). Rekkefølgen er praktisk begrunnet, ettersom artikkel 23 etter min vurdering er en mer aktuell begrensningshjemmel for det parlamentariske arbeidet enn artikkel 85 er.

1.3. Kravet til lovhjemmel

En felles forutsetning for anvendelse av de to bestemmelsene er at begrensningen eller unntatt er nedfelt i nasjonal lovgiving eller i EU-retten. Kravet til lovhjemmel må ses i lys av at artikkel 23 og artikkel 85 åpner for inngrep overfor den enkelte registrerte ved å begrense deres rettigheter etter GDPR.

Kravet om lovhjemmel har forskjellig utforming i de respektive bestemmelsene. GDPR artikkel 85 forutsetter at unntaket gjøres «by law», mens etter artikkel 23 skal begrensningen nedfelles «by way of a legislative measure». Likevel indikerer begge ordlydene at en

begrensning må følge av lov. I fortalepunkt (41) er det uttalt at «[w]here this Regulation refers to a legal basis or a legislative measure». Uttalelsen synes å forutsette at lovskravet i forordningen gjennomgående har det samme innholdet, selv om henvisningene er ulike.

Kravet til lovhjemmel har for det første en kvalitativ side. De respektive ordlydene i artikkel 23 og artikkel 85 gir ikke anvisning på hva som kvalifiserer som «law» og «legislative measure». Fortalepunkt (41) presiserer imidlertid at «this does not necessarily require a legislative act adopted by a parliament» og at det vesentlige er at hjemmelen er «clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of the European Union (the ‘Court of Justice’) and the European Court of Human Rights». Dermed er det ikke et absolutt krav at begrensningen er nedfelt i lov som er vedtatt av medlemsstatens lovgivende organ, så lenge hjemmelen er tilstrekkelig tilgjengelig og presis. Henvisningen til EU-domstolen og Den europeiske menneskerettighetsdomstolen (EMD) innebærer at lovskravet har en unison betydning i EU- og Europarådet.

Henvisningen i fortalepunkt (41) betyr også at en begrensning eller et unntak må overholde den grunnleggende skranken fastsatt i artikkel 52 nr. 1 i Den europeiske unions pakt om grunnleggende rettigheter («Charteret»). Bestemmelsen fastslår at enhver begrensning i rettigheter «recognised by this Charter» – inkludert retten til vern om personopplysninger jf. artikkel 8 – må nedfelles i lov og «respect the essence of those rights and freedoms». I den grad det gjøres begrensning må disse være i tråd med «the principle of proportionality» og «made only if they are necessary and genuinely meet the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others». Kravet samsvarer med lovskravet utpenslet i EMD-praksis. Hensikten med lovskravet er å beskytte borgerne mot vilkårlighet ved å forhindre at myndighetene i realiteten gis en «blankofullmakt» til inngrep.²⁴

²⁴ Se blant annet EMD sine uttalelser i *Malone mot Storbritannia* [1984] avsnitt 67.

Kravet om at unntaket eller begrensningen må forankres i lov innebærer også at forpliktelsen påhviler medlemsstatene, og ikke den enkelte «controller» jf. *Buivids [C2]*, C-345/17, avsnitt 51, og *Satakunnan Markkinapörssi and Satamedia [GC]*, C-73/07, avsnitt 56.²⁵ En «controller» kan med andre ord ikke selv begrense en forpliktelse eller rettighet ved å påberope artikkel 23 uten hjemmel i EU- eller nasjonal rett.

Lovskravet medfører derfor at eventuelle unntak etter artikkel 85 eller begrensninger etter artikkel 23 må gjøres av lovgiver og utformes i samsvar med de kvalitative kravene til tilgjengelighet og presisjon som følger av EU- og EMD-praksis. For personvernet innebærer dette at den nasjonale lovgivningen må ha vilkår som gir de registrerte en adekvat indikasjon på under hvilke omstendigheter og på hvilke vilkår deres rett til vern om personopplysninger kan innskrenkes. I konteksten av denne oppgaven vil lovskravet forhindre at de registrertes personopplysninger behandles vilkårlig av staten.

Norsk lovgivning inneholder per i dag ikke noen hjemmel som begrenser anvendelsen av enkelte bestemmelser i GDPR for det parlamentariske arbeidet – hverken helt eller delvis. Videre i oppgaven vil jeg derfor analysere i hvilken grad de respektive bestemmelsene *åpner for* begrensninger eller unntak for det parlamentariske arbeidet.

2. GDPR artikkel 85

2.1. Om bestemmelsen

²⁵ Se tilsvarende i *EDPB Guidelines 10/2020* (2020), s. 7

Som et utslag av at vernet om personopplysninger ikke er absolutt, åpner artikkel 85 for at medlemslandene gjennom nasjonal lovgivning og på nærmere vilkår kan gjøre unntak fra forordningen av hensyn til nærmere angitte formål innen ytrings- og informasjonsfriheten.

Artikkel 85 første ledd konstaterer at medlemslandene «by law» skal «reconcile the right to the protection of personal data pursuant to this Regulation» med «the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression».

Ved behandling av personopplysninger som faller inn under artikkel 85 nr. 1, stiller artikkel 85 nr. 2 ytterligere vilkår for et eventuelt unntak basert på bestemmelsen. Dersom et medlemsland skal kunne «provide for exemptions or derogations» fra nærmere angitte kapitler i forordningen, må dette være «necessary to reconcile the right to the protection of personal data with the freedom of expression and information». Forutsatt at vilkårene i artikkel 85 nr. 1 og nr. 2 er innfridd, åpner bestemmelsen opp for potensielt omfattende unntak fra forordningens rettigheter og plikter ved behandling av personopplysninger.

I den videre gjennomgangen skal jeg drøfte hvorvidt det parlamentariske arbeidet kan innfortolkes i artikkel 85. Et første spørsmål er hvordan «the right to freedom of expression and information» i nr. 1 skal forstås, herunder om «journalistic purposes and the purposes of academic, artistic og literary expression» er en uttømmende angivelse av relevante formål under ytrings- og informasjonsfriheten (2.2.). Deretter følger en vurdering av om artikkel 85 kan anvendes for å unnta det parlamentariske arbeidet (2.3.). Gjennomgangen under punkt 2.2. og 2.3. viser at det parlamentariske arbeidet etter min mening ikke kan innfortolkes i artikkel 85.

2.2. Er «journalistic purposes and the purposes of academic, artistic or literary expression» en uttømmende angivelse av hva som kan begrunne unntak av hensyn til ytrings- og informasjonsfriheten?

2.2.1. Ordlyd

Ordlyden «right to freedom of expression and information» gir anvisning på handlinger som angår retten til å uttrykke seg og utlevere det man ønsker, og få tilgang til informasjon. Retten til ytrings- og informasjonsfrihet er nedfelt i Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 10 og Den europeiske unions pakt om grunnleggende rettigheter (Charteret) artikkel 11, og anses som en grunnleggende rettighet. Isolert sett er dette vernet svært vidtrekkende.

Vilkåret må imidlertid tolkes i lys av konteksten det står i. Artikkel 85 nr. 1 konstaterer at personvernet må avveies mot ytrings- og informasjonsfriheten, «including» «processing for journalistic purposes and the purposes of academic, artistic or literary expression». Bruken av «including» indikerer en avgrensning av det vide vernet om ytrings- og informasjonsfrihet generelt. Uten en slik avgrensning vil rommet for unntak være svært omfattende, som følge av at ytrings- og informasjonsfriheten favner vidt. En vid unntaksadgang ville i praksis fort kunne uthule forordningens grunnleggende formål om å verne de registrertes personopplysninger.

Spørsmålet er derfor om «journalistic purposes or the purpose of academic, artistic or literary expression» er en uttømmende angivelse av formål innen ytrings- og informasjonsfriheten som kan begrunne unntak i medhold av artikkel 85 nr. 1, eller om angivelsen kun er en eksemplifisering av formål som et unntak kan baseres på.

Ordlyden «including» synes ikke å utelukke at også andre enn de nevnte formålene kan danne grunnlag for unntak. Vilkåret kan oversettes til «inkludert» på norsk, og dermed forstås som en eksemplifiserende henvisning.

Den danske versjonen av personvernforordningen, som også er autoritativ, bruker «herunder». I danske ordbøker er begrepet synonymt med «heri indbefattet», og betydningen eksemplifisert med at «en del plasticityper er farlige, herunder skumplast».²⁶ Den svenske bestemmelsen bruker «inbegripet», den franske bruker «y compris» og den tyske bruker «einschließlich». Ordlyden i disse ulike autoritative språkversjonene synes alle å samsvare med forståelsen av det engelske «including» og dermed som en løsere angivelse av relevante formål. Likevel gir ikke ordlydstolkningene et endelig svar på spørsmålet om formålene i artikkel 85 første ledd er oppgitt uttømmende eller ikke. Tolkningen av bestemmelsen må suppleres ved bruk av øvrige rettskilder.

2.2.2. Betydningen av endringer fra direktiv 95/46/EC

Det nå avløste direktiv 95/46/EC, som er forløperen til GDPR, hadde i artikkel 9 en tilsvarende unntaksbestemmelse for ytringsfriheten av hensyn til nærmere angitte formål. Etter direktivet artikkel 9 kunne unntak gjøres for aktiviteter som «solely» hadde journalistiske, kunstneriske eller litterære formål. For direktivet var rettstilstanden at oppramsingen var uttømmende, se blant annet *Satakunnan Markkinapörssi and Satamedia [GC]*, C-73/07, avsnitt 52.

Utformingen av GDPR artikkel 85 er noe annerledes enn direktivet artikkel 9, ettersom vilkåret «solely» er endret til «including» og forordningen også har innlemmet formålet «academic purposes» under ytrings- og informasjonsfriheten. Følgelig må det vurderes om rettstilstanden fortsatt er at bestemmelsen uttømmende angir hvilke aktiviteter som kan begrunne unntak av hensyn til yttings- og informasjonsfriheten, eller om endringen gjør at også andre aktiviteter kan innfortolkes i GDPR artikkel 85 nr. 1.

²⁶ Den Danske Ordbog, «herunder»

Basert på en alminnelig språkforståelse fremstår vilkåret «solely» som en strengere angivelse av aktiviteter enn «including», da ordlyden tilsier at behandlingen må skje *utelukkende* av hensyn til de angitte formål. Endringen kan derfor være uttrykk for et ønske om å åpne for at flere aktiviteter kan unntas på bakgrunn av ytrings- og informasjonsfriheten.

På den annen side kan innlemmelsen av «academic purposes» i GDPR artikkel 85 nr. 1 antyde en forutsetning om at oppramsingen er uttømmende. Direktivets bestemmelse åpnet ikke for unntak av hensyn til akademiske formål. Derfor kan den eksplisitte inntakelsen av akademiske formål tilsi en presumsjon om at unntaksberettigede formål må fremgå uttrykkelig av bestemmelsen.

Fortalen til GDPR adresserer ikke endringen i utformingen av direktivet artikkel 9 til GDPR artikkel 85. Dersom formålet var å endre rettstilstanden er det naturlig at dette ville vært kommentert i fortalen. At fortalen er taus om problemstillingen kan dermed tilsi at endringen ikke var tilsiktet innholdsmessig betydning for oppramsingens uttømmende karakter.

Det er ikke gitt avgjørelser fra EU-domstolen tilknyttet GDPR artikkel 85, og dermed har domstolen heller ikke behandlet betydningen av den endrede utformingen fra direktivet til forordningen. Likevel har EU-domstolen i *Satakunnan Markkinapörssi and Satamedia, C-73/07*, noen uttalelser som kan være relevante. Dommen ble avsagt før forordningen trådte i kraft, men etter arbeidet var påbegynt. Domstolen introduserte GDPR artikkel 85 som at den skulle «replace the journalistic purposes derogation in Article 9» (69). Uttalelsen indikerer at rettstilstanden etter direktivet artikkel 9 er ment videreført i GDPR artikkel 85.

I mangel på overnasjonale rettskilder kan praksis fra EU-landenes tilsynsmyndigheter få betydning i tolkningen av forordningen. Tolkningen gjort av nasjonale tilsynsorgan representerer imidlertid ikke en autoritativ forståelse av forordningen, og vekten er begrenset. Den norske personvernemndas vedtak 2. februar 2021, PVN-2020-19, kan likevel være relevant. Saken gjaldt innhenting og publisering av kredittopplysninger i en avisartikkel i

Bergens Tidene. Spørsmålet var om dette ble gjort utelukkende for journalistiske formål slik at det ikke var i strid med personopplysningsloven § 3²⁷. Siden bestemmelsen bygger på GDPR artikkel 85, uttaler nemda seg også om tolkningen av artikkel 85. Det er kun uttalelsene om forordningens artikkel 85 som er relevant for denne oppgaven.

Personvernemda uttaler at GDPR artikkel 85 i det vesentlige sammenfaller med 95-direktivet artikkel 9, og legger til grunn at rettspraksis knyttet til sistnevnte fortsatt har relevans. Tilsvarende viderefører den norske gjennomføringen av GDPR, personopplysningsloven, rettstilstanden etter personopplysningsloven 2000 § 7 som gjennomførte EUs direktiv 95/46/EC. I den forbindelse henviser nemda til personopplysningslovens forarbeider²⁸ i kap. 38.1 og 14.2. Punkt 14.2 i forarbeidene påpeker blant annet at forordningens ordlyd ikke lenger krever behandling av personopplysninger som *utelukkende* forfølger et av de nevnte formålene som skal omfattes av unntaksregelen. Utvalget mener likevel det «neppe [er] grunn til å anta at forordningen artikkel 85 medfører noen endring på dette punktet», med henvisning til at forordningen i avsnitt 153 enda bruker formuleringen «utelukkende» («solely») ved angivelsen av formålene som kan unntas fra bestemmelsen. Det må understrekes forarbeidsuttalelsen har minimal vekt for tolkningen av GDPR. For det første er forarbeidene til den norske gjennomføringen av GDPR, personopplysningsloven, ikke en rettskilde på hvordan *forordningen* skal tolkes. I tillegg er den aktuelle uttalelsen ikke referert av nemda i tolkningen av GDPR artikkel 85, noe som svekker betydningen ytterligere. Slutningen og begrunnelsen er likevel interessant.

Videre, dersom formålene nevnt i artikkel 85 nr. 1 ikke tolkes uttømmende, vil bestemmelsen i realiteten åpne for en vidtrekkende unntaksadgang. Ettersom vernet om ytrings- og informasjonsfriheten strekker så vidt, er det behov for en fullstendig presisering av hvilke formål derunder som legitimt kan begrunne unntak eller en begrensning. Enkle omgørelser kan undergrave det grunnleggende formålet med GDPR om å gi de registrerte vern om personopplysninger.

²⁷ Formuleringen i den norske personopplysningsloven § 3 er endret i etterkant av Personvernemdas sak. Likevel er endringen i ordlyden av den norske bestemmelsen ikke av rettskildemessig betydning for tolkningen av artikkel 85, da det er nemdas uttalelser om GDPR artikkel 85 som er relevant for drøftelsen.

²⁸ Prop.56 LS (2017-2018)

Heller kan endringen i ordlyden forklares med henblikk på rettspraksis til direktivet artikkel 9. Kravet om «solely» innebar en forutsetning om at personopplysningene var behandlet *kun* for journalistiske, kunstneriske eller litterære formål. Dermed kom direktivet til anvendelse dersom behandlingen delvis hadde andre formål, se uttalelsene i *Buivids* (62). Domstolen uttalte at vilkåret «solely» fordret at behandlingen utelukkende hadde som formål å publisere informasjon, meninger eller ideer til offentligheten (jf. også *Satakunnan Markkinapörssi and Satamedia*, avsnitt 62). Dermed kunne unntak fra direktivet kun gjøres i de tilfeller der behandlingen av personopplysninger ene og alene var av hensyn til formålene nevnt i bestemmelsen.

På bakgrunn av dette kan den endrede ordlyden fra direktivet artikkel 9 til GDPR artikkel 85 tilsi at unntak kan gjøres i tilfeller der behandlingen har (bi)formål *i tillegg til* de som er eksplisitt nevnt i bestemmelsen. En slik forståelse er praktisk ettersom det kan være vanskelig å avgjøre grensedragningen for om noe utelukkende ment å fremme et journalistisk, akademisk, kunstnerisk eller litterært formål. Forutsetningen er likevel at behandlingen kan forankres i den uttømmende angivelsen av formål.

En tilsvarende forståelse synes å ligge til grunn for personopplysningsloven § 3, særlig etter endringen av bestemmelsens ordlyd.²⁹ Som nevnt har den norske gjennomføringen ikke rettskildemessig vekt for tolkningen av forordningen, men den gir et interessant eksempel på tolkningen av artikkel 85. Personopplysningsloven § 3 er nå vedtatt med en annen ordlyd, da unntak fra forordningen kan gjøres «så langt det er nødvendig» av hensyn til de opplistede formålene. Uttalelser i forarbeidene indikerer forutsetningsvis at oppramsingen er uttømmende.³⁰ Det står videre på s. 44 at «det er ikke et vilkår etter første ledd at behandlingen utelukkende skjer for et av de angitte formålene» men at slik behandling i alminnelighet vil ha sterkere vern «enn behandlinger som samtidig har andre formål».

²⁹ Jf. Prop. 158 L (2020-2021)

³⁰ Prop. 158 L (2020-2021) s. 44

Selv om utformingen av GDPR artikkel 85 er endret fra direktivet artikkel 9, anses rettstilstanden som videreført i den forstand at bestemmelsen uttømmende angir hvilke aktiviteter som kan begrunne unntak av hensyn til ytings- og informasjonsfriheten.

2.2.3. Oppsummering

Samlet sett taler rettskildene for at endringen i ordlyden fra direktivet artikkel 9 til GDPR artikkel 85 nr. 1 ikke innebærer en endring av bestemmelsens uttømmende karakter. Følgelig er det kun adgang til å gjøre unntak etter artikkel 85 nr. 1 for «journalistic purposes and the purposes of academic, artistic or literary expression». Dette samsvarer også med formålet om at GDPR skal gi et utstrakt vern om personopplysninger.

Bestemmelsen i artikkel 85 tolkes som å uttømmende angi hvilke formål innen yttings- og informasjonsfriheten som kan begrunne unntak.

Forutsatt at formålene nevnt i artikkel 85 *ikke* er uttømmende, er det heller ikke gitt at bestemmelsen omfatter behandling av personopplysninger i det parlamentariske arbeidet. Oppgavens omfang gjør det imidlertid nødvendig å avgrense mot en slik subsidiær drøftelse.

2.3. Kan behandlingen av personopplysninger i det parlamentariske arbeidet unntas etter artikkel 85?

2.3.1. Ordlyd

GDPR artikkel 85 nr. 1 angir uttømmende hvilke formål innen yrings- og informasjonsfriheten som kan begrunne unntak fra forordningen. Av disse formålene er det «journalistic purposes» som fremstår mest relevant for vurderingen av om det parlamentariske arbeidet kan innfortolkes.

Vilkåret «journalistic» indikerer at man opptrer i yrket som journalist. Journalisme innebærer å formidle meninger og saker i offentligheten, og formålet med utøvelsen må sies å i stor grad forutsette grad yrings- og informasjonsfrihet. Journalister utøver en kontrollfunksjon og betegnes i Norge uoffisielt som «den fjerde statsmakt»³¹. Selv om utøvelse av journalistiske formål kan medføre behandling av personopplysninger, kan viktigheten av å publisere den konkrete saken være avgjørende for å ivareta kontrollfunksjonen. Særlig kan denne utøvelsen være utsatt for inngrep og sensur fra myndighetene. Det kan dermed være tungtveiende grunnleggende rettigheter som tilsier at vern om personopplysninger må vike for kravet til yrings- og informasjonsfriheten.

2.3.2. Fortalepunkt (153)

Fortalepunkt (153) konstaterer at det er «necessary to interpret notions relating to that freedom, such as journalism, broadly» for å ta høyde for viktigheten av retten til yrings- og informasjonsfriheten. Uttalelsen gir derfor rom for å tolke «journalistic» noe videre enn ordlyden først gir inntrykk av.

2.3.3. Rettspraksis

EU-domstolen har ikke uttalt seg om forståelsen av de aktuelle formålene i GDPR artikkel 85. Rettspraksis knyttet til direktivet kan imidlertid gi tolkningsbidrag, ettersom innholdet i

³¹ Orgeret (2020).

GDPR artikkel 85 viderefører direktivet artikkel 9 jf. *Satakunnan Markkinapörssi and Satamedia [GC]*, C-73/07, avsnitt 69.

EU-domstolens avgjørelse i *Buivids [C2]*, C-345/17, omhandlet et videoopptak gjort av herr Buivids på en politistasjon hos det latviske politiet. I videoen, som ble publisert på nettstedet Youtube, protesterte Buivids mot straffen han ble ilagt på stasjonen mens han filmet to politimenn. Et av spørsmålene i saken var om det kunne gjøres unntak fra 95-direktivet etter artikkel 9. Argumentet var at Buivids i medhold av ytringsfriheten publiserte videoen for å gjøre allmenheten oppmerksom på noe han mente var ulovlig myndighetsutøvelse fra politiets side. EU-domstolen foretok ikke noen subsumsjon, men kom til at bestemmelsen åpnet for unntak i en slik situasjon dersom vilkårene var innfridd.

Domstolen understreket i avsnitt 51 at vilkåret «journalism» må tolkes bredt for å kunne ta høyde for viktigheten av ytrings- og informasjonsfriheten. I denne forbindelse ble det uttalt at 95-direktivet artikkel 9 skulle «apply not only to media undertakings but also to every person engaged in journalism». Følgelig er det ikke avgjørende at man opererer som profesjonell journalist. Dette kan ses i lys av utviklingen av digitale plattformer som har gjort at spredningen av informasjon i den offentlige debatten – og til en viss grad rollen som «public watchdog» – ikke lenger er begrenset til tradisjonell presse.³² Med henvisning til øvrige avgjørelser fra EU-domstolen uttalte domstolen også at «journalistic activities» omfatter «those which have as their purpose the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them» i avsnitt 53. Dette betyr likevel ikke at «all information published on the internet, involving personal data, comes under the concept of 'journalistic activities' and thus benefits from the exemptions and derogations provided for in Article 9 of Directive 85/45» jf. avsnitt 58. Uttalelsene synes å forutsette at formidlingen er gjort for å avdekke noe, og at viktigheten av dette begrunner en eventuell begrensning i retten til vern om personopplysninger. Hvilket medium informasjonen blir formidlet gjennom er likevel ikke avgjørende.

³² Poenget er også fremhevet av EMD i tolkningen av EMK artikkel 10 om retten til vern om ytringsfriheten, se, *Magyar Helsinki Bizottság mot Ungarn* [2016] avsnitt 166–168

Videre uttalte domstolen at «solely [...] for journalistic purposes» betyr at innspillingen og publiseringen var ment *utelukkende* å avsløre informasjon, meninger eller ideer til offentligheten jf. *Satakunnan Markkinapörssi and Satamedia* avsnitt 62. Publiseringen kunne ikke ha andre sideformål enn dette. Det sentrale var dermed at publiseringen hadde et budskap som er av allmenn interesse å avdekke, og at aktiviteten kun var gjort med henblikk på å spre dette budskapet.³³

EU-domstolen understreker i avsnitt 63 at unntak kun kan gjøres der det er «necessary in order to reconcile two fundamental rights, namely the right to privacy and the right to freedom of expression» og at det må være proporsjonalt i den forstand at det «must apply only in so far as is strictly necessary». Bemerkningen bygger på vilkårene i artikkel 85 nr. 2. For denne vurderingen viste domstolen I avsnitt 66 til momenter fra Den europeiske unions domstol (CJEU) og Den europeiske menneskerettighetsdomstolen (EMD), blant annet «the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and the manner and circumstances in which the information was obtained and its veracity». I tillegg må «the possibility for the controller to adopt measures to mitigate the extent of the interference with the right to privacy [...] be taken into account» jf. avsnitt 66.

Uttalelsene i *Buivids* og øvrig rettspraksis knyttet til tolkningen av «journalistic purposes» etter 95-direktivet artikkel 9 er relevant for forståelsen av det likelydende vilkåret i artikkel 85 nr. 1. Basert på fortalepunkt (153) og rettspraksis tolkes vilkåret «journalistic purposes» videre enn utøvelsen av *yrket* som journalist. Formålet med formidlingen må likevel være å avsløre informasjon, meninger eller ideer. Et unntak kan kun gjøres i den grad det er nødvendig og proporsjonalt.

³³ Som nevnt over i punkt 2.2.2. kan det imidlertid reises spørsmål om *forordningen* stiller tilsvarende krav om at formidlingen må skje utelukkende av hensyn til formålet, jf. endringen til vilkåret «including».

Spørsmålet er om det parlamentariske arbeidet er en utøvelse av hensyn til «journalistic purposes» som tilsier at det er «necessary» å gjøre unntak fra GDPR jf. artikkel 85.

Ytrings- og informasjonsfrihet er en viktig del av stortingsrepresentantenes virke. Arbeidet er demokratisk forankret og av allmenn interesse, og omfatter oppgaver som søker å spre et budskap til offentligheten. Det parlamentariske arbeidet formidler imidlertid ikke informasjon, meninger eller ideer for å *avdekke* eller *avsløre* noe slik «journalistic purposes» tar sikte på.

I tillegg er det problematisk hvis «journalistic purposes» tolkes så utvidende at det i realiteten omfatter enhver formidling av et budskap. En vid unntaksadgang svekker formålet om å gi et utstrakt vern til de registrerte – hvilket er det bærende hensynet bak forordningen. For å unngå en utvanning av bestemmelsen, må en utvidelse av den innholdsmessige forståelsen forankres på europeisk nivå. Samlet sett er det ikke holdepunkter for en slik forståelse, og følgelig synes ikke det parlamentariske arbeidet å innebærer en form for formidling som det artikkel 85 og «journalistic purposes» tar sikte på.

For å gjøre unntak må det dessuten anses «necessary to reconcile the right to the protection of personal data with the freedom of expression and information» jf. artikkel 85 nr. 2.

Bestemmelsen forutsetter altså at unntaket fra GDPR må være forholdsmessig. Den konkrete vurderingen må blant annet ta hensyn til hvor viktig arten og innholdet av nyheten er, hvordan den ble innhentet, og i hvilken grad behandlingsansvarlig kan avbøte inngrepet overfor den registrerte.³⁴ Dette forutsetter en konkret vurdering som i seg selv vanskeliggjør et generelt unntak for det parlamentariske arbeidet i sin helhet.

På denne bakgrunn kan behandlingen av personopplysninger i det parlamentariske arbeidet ikke anses utført av «journalistic purposes and the purposes of academic, artistic or literary

³⁴ Jf. momentene gjengitt i *Buivids* avsnitt 66 fra CJEU- og EMD-praksis.

expression» som gjør det «necessary» med et unntak for å «reconcile the right to the protection of personal data with the freedom of expression and information» jf. artikkel 85.

2.3.4. Danmarks tilnærming

Rapporten som er innhentet av parlamentet i Østerrike viser at Danmark ikke gir GDPR anvendelse på det parlamentariske arbeidet. En utredning fra det danske justitsministeriet³⁵ viser at de mener GDPR artikkel 85 åpner for unntak for det parlamentariske arbeidet.

Etter Danmarks utredning pålegger artikkel 85 medlemsstatene en «forpligtelse til at foretage en afvejning af disse to hensyn og fastsette nationale regler herom», og bruken av vilkåret «heunder» tolkes som at «anvendelsesområdet for artikkel 85 ikke er begrænset til behandling i journalistisk øjmed og med henblik på akademisk, kunstnerisk eller literær virksomhed».³⁶ Uttalelsene tyder på at Danmark tolker artikkel 85 som å åpne for unntak av hensyn til ytringsfriheten mer generelt – jf. formuleringen «afvejning af disse to hensyn» – og at opplistingen av formål ikke er uttømmende. Tolkningsspørsmålene er behandlet under punkt 2.2 og 2.3 i denne oppgaven.

Danmarks utredning viser også til fortalepunkt (153) og uttalelsene om at det er «nødvendigt at tolke begreber vedrørende ytringsfriheden, herunder f.eks. journalistik, bredt».³⁷ Gjennomgangen i punkt 2.4 adresserer dette forholdet.

Utredningen kommenterer også nødvendighetsvurderingen som artikkel 85 nr. 2 pålegger medlemsstatene ved gjennomføringen av unntak gjennom nasjonal lovgivning. Denne tolkes som en avveining mellom retten til personvern og ytrings- og informasjonsfriheten «med henblik på at sikre, at forordningens regler ikke unødigt medfører innskærpkninger i disse

³⁵ Danske justitsministeriet, nr. 1565

³⁶ Danske justitsministeriet, nr. 1565 s. 955

³⁷ Danske justitsministeriet, nr. 1565 s. 956

rettigheter»³⁸. På bakgrunn av dette anses unntakene som er nedfelt i den nasjonale persondataloven som «uttrykk for en konkret afvejning i dansk ret af hensynet til beskyttelse af personoplysninger på den ene side og hensynet til informations- og ytringsfrihed på den anden side». Danmark viser til avveiningene som ble foretatt i forbindelse med implementeringen av direktivet, og at rettstilstanden «kan videreføres» og være i samsvar med GDPR artikkel 85. De så dermed ikke grunn til å endre den nasjonale lovgivningen etter vedtakelsen av GDPR.

Samlet sett mener Danmark at det «af hensyn til informations- og ytringsfriheden [...] [vil] være muligt at fastsætte undagelser og fravigelser fra forordningen, for så vidt angår Folketingets medlemmers behandling af personoplysninger»³⁹. Begrunnelsen bygger på en generell avveining av hensynet til personoplysninger og hensynet til ytrings- og informasjonsfrihet. Avveiningen må knyttes konkret opp mot det parlamentariske arbeidet for å begrunne unntak. Omfanget av unntaksregler som anvendes, og nødvendigheten av disse, adresseres ikke i den offentlige utredningen.

3. GDPR artikkel 23

3.1. Om bestemmelsen

Bestemmelsen i GDPR artikkel 23 åpner for at medlemslandene gjennom nasjonal lovgivning og på nærmere angitte vilkår kan gjøre *begrensninger* i rettigheter og plikter som forordningen gir.

³⁸ Danske justitsministeriet, nr. 1565 s. 957

³⁹ Danske justitsministeriet, nr. 1565, s. 958

Artikkel 23 åpner for at unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige eller databehandleren er underlagt, kan «restrict by way of a legislative measure» rekkevidden av forpliktelsene og rettighetene som er fastsatt i artikkel 12—22 og som omhandler den registrertes rettigheter, artikkel 34 som angår underretning til den registrerte om brudd på personopplysningssikkerheten og artikkel 5 om personvernprinsippene i den grad dens bestemmelser svarer til rettighetene og pliktene som er fastsatt i artikkel 12—22. Forutsetningen for å begrense forordningens virkeområde er at begrensningen «respects the essence of the fundamental rights and freedoms» og er et «necessary and proportionate measure in a democratic society» for å sikre nærmere angitte formål som fremgår av artikkel 23 nr. 1 bokstav (a) til (j). Artikkel 23 nr. 2 gir vilkår med innholds- og formkrav til en eventuell lovbestemmelse. Vilkårene er kumulative – de må alle være innfridd for at en begrensning skal kunne finne sted.

Innholdet i vilkåret om «legislative measure» er behandlet under punkt 1.3. Den videre fremstillingen vil først ta for seg det rettslige innholdet i angivelsen av de konkrete formålene som kan hjemle en begrensning (3.2.), og deretter vilkårene «restriction» (3.3.), «respect the essence of the fundamental rights and freedoms» (3.4.) og «necessary and proportionate measure in a democratic society [...]» (3.5.). Basert på den rettslige gjennomgangen av vilkårene i artikkel 23, vil punkt 4 undersøke hvordan det parlamentariske arbeidet kan subsumeres under bestemmelsen.

3.2. De angitte formålene som kan hjemle en begrensning

GDPR artikkel 23 forutsetter at ett eller flere av de angitte formål i første ledd bokstav (a) til (j), gjør det «necessary and proportionate» å vedta en begrensning i vernet om personopplysninger gjennom lov.⁴⁰ European Data Protection Board (EDPB) er EU sitt Personvernråd, og har utgitt en veiledning for tolkningen av artikkel 23 som uttaler at «[t]his list is exhaustive, meaning restrictions cannot be carried out under any other conditions than

⁴⁰ Innholdet i vilkåret «necessary and proportionate [...]» behandles i punkt 3.5.

the ones listed [...]”.⁴¹ Videre uttaler EDPB at tilknytningen mellom begrensningen og formålet den forankres i «should be clearly stated in the legislative measure». Følgelig er listen med formål uttømmende, og forankringen må fremgå tydelig.

Flere av formålene som er nedfelt i artikkel 23 fremgår også av artikkel 2 nr. 2 som omhandler begrensningen av forordningens virkeområde. Dette gjelder blant annet «national security» og «defence». Karakteristikkene ved disse områdene kan tilsa at vernet etter GDPR bør vike for å skjerme andre beskyttelsesverdige interesser fra eksempelvis tilgangen til informasjon om hvilke opplysninger som behandles. Forskjellen mellom artikkel 2 nr. 2 og 23, er at artikkel 2 nr. 2 avgrenser *hele* forordningen og alle dens bestemmelser fra gitte *områder*, og omfanget er dermed omfattende. Bruken av artikkel 23 innebærer imidlertid at forordningen i utgangspunktet kommer til anvendelse for behandlingen av personopplysninger for de aktuelle områdene, men at det etter en konkret vurdering gjøres begrensninger i forordningens virkeområde i tråd med vilkårene. Vurderingen etter artikkel 23 angår således myndigheten til å innføre begrensninger i *konkrete situasjoner* innen det gitte området for å ivareta et bestemt hensyn.

Hvilke av de opplistede formålene som kan være relevante for en begrensning av hensyn til det parlamentariske arbeidet vil bli kommentert nedenfor i punkt 4.2. og 4.3. Først gir punkt 3.3. til 3.5. en overordnet gjennomgang av det rettslige innholdet i vilkårene etter artikkel 23.

3.3. «[R]estriction»

Vilkåret «restriction» gir adgang til å innskrenke rettigheter og plikter slik at de ikke lenger gjelder fullt ut. Ordlyden gir ikke anvisning på en bestemt størrelse for begrensningen. Likevel understreker EDPB i sine retningslinjer at artikkel 23 ikke gir hjemmel for å begrense

⁴¹ EDPB Guidelines 10/2020 (2020) s. 8.

beskyttelsen av personopplysninger i sin helhet – de grunnleggende rettsprinsippene må til enhver tid overholdes.⁴² For eksempel kan ikke en begrensning gjøres irreversibel.

Artikkel 23 lister konkrete bestemmelser hvis anvendelse kan begrenses dersom vilkårene er innfridd. Artiklene 12–22 inngår i kapittel III, «[r]ights of the data subject». Her er den registrertes rettigheter spesifisert og kategorisert særlig for ulike type situasjoner – se eksempelvis reglene om innsyn (art. 15), retting (art. 16), sletting (art. 17) og rett til å protestere (art. 21). Bestemmelsene gir i hovedsak den registrerte rett til å stille ulike krav til den som er «controller» etter artikkel 4 nr. 2.

Hjemmelen i artikkel 23 gir også adgang til å begrense artikkel 34, som omhandler plikten til å underrette den registrerte om brudd på personopplysningssikkerhet der denne er «likely to result in a high risk to the rights and freedoms of natural persons». Etter fortalepunkt (86) er hensikten å gi den registrerte mulighet til å treffe nødvendige forholdsregler. Plikten for «controller» utløses uten at den registrerte selv påberoper seg rettigheten.

Begrensningsadgangen etter artikkel 23 omfatter også noen av personvernprinsippene i GDPR artikkel 5. En viktig bemerkning er at artikkel 5 kun kan begrenses i den grad prinsippene samsvarer med rettighetene og forpliktelsene gitt i artikkel 12–22. Eksempelvis kan en begrensning i retten til informasjon om formålet med innhenting etter artikkel 13 nr. 1 bokstav (c) også tenkes å innebære en begrensning i prinsippet om at opplysningen er innhentet for «explicit [...] purposes» som er tydeliggjort overfor den registrerte jf. artikkel 5 nr. 1 bokstav (b). Dermed åpner artikkel 23 for et innhugg i noen av de prinsippene som forordningen bygger på.

Artikkel 23 nr. 2 – som angir formkrav til en eventuell begrensning av forordningen – stiller samtidig krav som langt på vei samsvarer med prinsippene nedfelt i artikkel 5. Bestemmelsen tolkes som et utslag av lovskravet. Dermed kan det hevdes at selv om prinsippene i artikkel 5

⁴² EDPB Guidelines 10/2020 (2020), s. 5.

innskrenkes, så skal den aktuelle lovgivningen hovedsakelig speile de samme hensyn som motiverer flere av prinsippene.⁴³

3.4. «[R]espect the essence of the fundamental rights and freedoms»

3.4.1. Ordlyd

Vilkåret «respect the essence of the fundamental rights and freedoms» uttrykker en grunnleggende skranke. Lovhjemmelen må overholde de underliggende rettighetene som forordningen skal sikre. Formuleringen skiller ikke mellom krav til innhold og utforming, og tolkes derfor som å omfatte begge aspekter. Det vesentlige er å forhindre at lovhjemmelen i realiteten uthuler retten til vern om personopplysninger.

Kravet kan også ses i sammenheng med at begrensningsadgangen etter artikkel 23 knyttes til konkrete bestemmelser (innhold), og de formelle kravene nedfelt i artikkel 23 nr. 2 om formuleringen av en eventuell nasjonal lovgivning (utforming). Skrankene bidrar til at utformingen av en begrensning ikke kan bli for omfattende.

3.4.2. Rettspraksis

EU-domstolen har kommentert hva som menes med essensen i personvernet, blant annet i *Digital Rights Ireland [GC]*, C-293/12, avsnitt 38—40. Dommen omhandler lovligheten av direktiv 2006/24/EC i lys av Charteret artikkel 52, jf. artikkel 7 og 8. Direktivet påla internett-

⁴³ Wiese Schartum, *Personvernforordningen* (2020) s. 88

tjenesteleverandører (ISP) å lagre telekommunikasjonsdata for å lette nasjonale myndigheters forebygging og forfølgelse av kriminalitet.

I avsnitt 40 drøfter EU-domstolen blant annet innholdet i «the essence of the fundamental right» til «the protection of personal data» jf. Charteret artikkel 52 jf. artikkel 8, og uttalelsene har betydning for tolkningen av det samsvarende vilkåret i GDPR artikkel 23. Det aktuelle direktivet var et inngrep i retten til vern om personopplysninger etter Charteret artikkel 8, men utgjorde likevel ikke en *krenkelse* av «the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter». Begrunnelsen var at den aktuelle inngrepshjemmelen «provides that [...] certain principles of data protection and data security must be respected by providers of publicly available electronic communications networks», og at disse påla medlemsstatene å «ensure that appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data» jf. avsnitt 40. Avgjørende var dermed at direktivet påla leverandørene å respektere visse prinsipper for databeskyttelse og datasikkerhet, og å implementere passende tekniske og organisatoriske tiltak for å ivareta dette formålet.

Selv om essensen i personvernet var overholdt, konkluderte EU-domstolen likevel med at direktivet ikke overholdt «the principle of proportionality» jf. Charteret artikkel 52. Direktivet var dermed rettsstridig. Bakgrunnen for denne konklusjonen var særlig omfanget av telekommunikasjonsmidler og kretsen av personer som ble rammet.

3.4.3. EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR

EDPB har som nevnt publisert retningslinjer knyttet til tolkningen og håndhevelsen av artikkel 23. Som eksempel på en begrensning som ikke overholder vilkåret, nevner retningslinjene generelle utelukkelse av registreres rettigheter med hensyn til alle eller

spesifikke databehandlingsoperasjoner, eller med hensyn til spesifikke behandlingsansvarlige.⁴⁴

Veiledningen forstås som at dersom begrensningen blir utformet for vidt, vil det i realiteten undergrave «the essence of the fundamental rights and freedoms» til personopplysninger fordi adgangen til å gjøre unntak blir for omfattende. EDPB skriver også at dersom en rettighet må anses for å være kompromittert, er tiltaket ugyldig uten at en behøver å vurdere de øvrige vilkårene i bestemmelsen om nødvendighet og forholdsmessighet.

3.5. «[N]ecessary and proportionate measure in a democratic society to safeguard» de nærmere angitte formålene

Ordlyden «necessary and proportionate» tilsier at den aktuelle begrensningen må være relevant og forholdsmessig. Fortalepunkt (73) uttaler at begrensningene «should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms». Uttalelsen signaliserer at vilkåret må tolkes i lys av EU- og EMD-praksis.

Målestokken for hva som er «necessary» synes etter ordlyden å basere seg på en avveining mellom behovet for å sikre et av formålene som er nevnt i bestemmelsen, og behovet for vern om personopplysninger i det konkrete tilfellet. EDPB presiserer i sine retningslinjer at det er «the objective of general interest» som danner grunnlaget for en slik nødvendighetsvurdering. Angivelsen forstås som at det må påvises en allmenn interesse i å ivareta et av de opplistede formålene i bestemmelsen.

⁴⁴ EDPB Guidelines 10/2020 (2020), s. 6. Uttalelsen kan tilsi at en begrensning av hensyn til «det parlamentariske arbeidet» vil være for generelt utformet. Dette poenget behandles nærmere i punkt 4.3.

En vurdering av om begrensningen er «proportionate» forutsetter at kravene til nødvendighet er oppfylt.⁴⁵ EDPB sine retningslinjer viser til at «the content of the legislative measure cannot exceed what is strictly necessary to safeguard the objectives listed in Article 23(1)(a) to (j) GDPR». Selv om begrensningen anses nødvendig, så må den altså avgrenses til det som er «strictly necessary». Dette samsvarer med EU-domstolens generelle uttalelser om at «derogations and limitations in relation to the protection of general data [...] must apply only insofar as is strictly necessary» jf. (56) i *Satakunnan Markkinapörssi and Satamedia*, C-73/07. Bestemmelsen krever også at proporsjonaliteten begrunnes konkret, og at begrensningen «will need to focus on specific risks». Som eksempel uttales det at dersom det vedtas begrensninger av hensyn til offentlig helse i et nødtilfelle, må begrensningen være strengt avgrenset i tid og omfang – og kun opprettholdes så lenge nødsituasjonen vedvarer.

Vilkårene legger opp til en streng vurdering både av hvorvidt begrensningen er nødvendig, og hvorvidt omfanget av begrensningen er proporsjonalt gitt inngrepet overfor den registrerte.

4. GDPR artikkel 23 og det parlamentariske arbeidet

4.1. Innledende

Som nevnt i punkt 1.3. er vilkåret «legislative measure» en henvisning til lovskravet, og innebærer blant annet at en begrensning etter artikkel 23 må vedtas av lovgiver. Norske lovgivere har foreløpig ikke vedtatt noen hjemmel som begrenser anvendelsen av enkelte bestemmelser i GDPR for (deler av) det parlamentariske arbeidet.

Den videre drøftelsen skisserer hvorfor og hvordan artikkel 23 kan være en aktuell begrensningshjemmel av hensyn til det parlamentariske arbeidet. Gjennomgangen viser typen

⁴⁵ EDPB Guidelines 10/2020 (2020), s. 10

parlamentarisk arbeid som kan aktualisere behovet for en begrensning og hvordan begrensningen kan utformes (4.2. og 4.3.). Deretter gis alternativer i norsk lovgivning hvor en begrensning kan hjemles (4.4.). Betraktningene gis *de lege ferenda*.

Alternativene som følger av de neste punktene gir ikke svar på tolkningen av forordningens vilkår om blant annet «controller» og «processor», eller hvem som skal ha myndighet som «supervisory authority», jf. artikkel 4 nr. 7, nr. 8 og nr. 21. De neste drøftelsene forutsetter derfor at vilkårene er innfridd. Likevel vil det i del IV punkt 1.1 og 1.2. gis betraktninger til vilkårene «controller» og «supervisory authority» i tilknytning til det parlamentariske arbeidet, i forbindelse med hva som bør avklares ved en eventuell lovendring.

4.2. Om det parlamentariske arbeidet

En sentral del av Stortingets arbeid er å fatte vedtak, og vedtakene er basert på forslag fra en av Stortingets faste komiteer.⁴⁶ Komiteene utgjør dermed Stortingets saksforberedende organer, og det er her den detaljerte saksbehandlingen finner sted. Komiteenes møter foregår bak lukkede dører. Det er ikke adgang til å gjengi andres uttalelser fra et lukket komitémøte, og protokollen som skrives er heller ikke offentlig. Hensikten med dette er å skape «politiske verksteder» der medlemmene kan tale fritt og diskutere seg frem til kompromisser på tvers av politiske skillelinjer.⁴⁷ Arbeidet i komiteene resulterer så i en komitéinnstilling som legges frem for Stortinget, og denne innstillingen er offentlig.

I spesielle tilfeller kan Stortingets presidentskap fremme innstilling om å nedsette særskilte komiteer til å behandle en enkelt sak eller saker av et bestemt slag⁴⁸. Adgangen til å nedsette slike komiteer benyttes relativt sjelden⁴⁹, men ble blant annet gjort i 2020 for å behandle saker

⁴⁶ Stortinget, «Fagkomiteene»

⁴⁷ Stortinget, «Komitéarbeidet»

⁴⁸ Se Stortingets forretningsorden § 18.

⁴⁹ Grimstad, *Stortingets forretningsorden med kommentarer*, kommentar til § 18

i forbindelse med koronakrisen⁵⁰ og i 2011 etter terrorangrepet 22. juli og det påfølgende arbeidet med styrket beredskap og økt sikkerhet⁵¹. *Ad hoc*-preget ved de særskilte komiteene gjør at Stortinget kan ta stilling til og prioritere saker av ekstraordinær karakter.

Som drøftelsen av artikkel 2 viste⁵², er utgangspunktet at GDPR gjelder for det parlamentariske arbeidet. Dette gjelder også komitéarbeidet, selv om det saksforberedende arbeidet her skjer bak lukkede dører og den offentlige innstillingen bygger på saksdokumenter som ikke er offentlige. Dermed må personopplysninger som eventuelt behandles i tilknytning til komiteenes arbeid skje i tråd med forordningen.

På tross av utgangspunktet om at GDPR gjelder, vil den videre gjennomgangen illustrere situasjoner innen det parlamentariske arbeidet der artikkel 23 kan være relevant for å begrense rettighetene og pliktene etter GDPR. Hensikten med fremstillingen er å eksemplifisere praktiske tilfeller. Det rettslige innholdet av formålene som begrensningen må være forankret i vil derfor ikke behandles inngående.

4.3. Begrensning gjennom artikkel 23

Den rettslige gjennomgangen av vilkårene i artikkel 23 viste blant annet at en begrensning av de registrertes rettigheter i medhold av bestemmelsen ikke kan være for generell og omfattende.⁵³ Denne forutsetningen tyder på at en eventuell begrensning av hensyn til det parlamentariske arbeidet må spesifiseres og avgrenses.

⁵⁰ Referat fra stortingsmøte 16. mars 2020

⁵¹ Innst. 207 S (2011-2012)

⁵² Del II punkt 2

⁵³ Se særlig vilkåret «respect the essence of the fundamental rights and freedoms»

I rapporten innhentet av parlamentet i Østerrike har enkelte land gitt forslag til hvordan eventuelle begrensninger etter artikkel 23 kan ta form. Forslagene kan være en inspirasjonskilde for norsk lovgivning.

Alle forslagene er imidlertid ikke aktuelle. Kypros og Ungarn gir GDPR anvendelse, og knytter spørsmålet om behandling av personopplysninger i det parlamentariske arbeidet opp mot kravene til behandlingsgrunnlag i GDPR artikkel 6 nr. 1 bokstav (c) eller (e) sammenholdt med nr. 3, og artikkel 9 nr. 2 bokstav (g). Løsningen synes lite hensiktsmessig ettersom problemstillingen ikke er hvorvidt behandling av personopplysninger i det parlamentariske arbeidet er *lovlig* eller ikke, jf. artikkel 6. Hvilket grunnlag behandlingen forankres i, bidrar hverken til å avklare spørsmålet om GDPR kommer til anvendelse, eller om anvendelsen av forordningen kan begrenses for det parlamentariske arbeidet – enten helt eller delvis.

Rapporten nevner også at Irland – som mener det parlamentariske arbeidet faller utenfor GDPR sitt anvendelsesområde etter artikkel 2 nr. 2 – har inntatt en generell begrensning i nasjonal lovgivning av de registrertes rettigheter som tilsvarer utformingen av GDPR artikkel 23. Data Protection Act 2018 seksjon 69 nr. 1 bokstav (a) og nr. 3 bokstav (a)(i) åpner for at rettighetene som fremgår av artikkel 12—22 på nærmere vilkår kan begrenses av hensyn til «parliamentary privilege». Vilkåret er ikke nærmere omtalt i rapporten eller i den irske lovens forarbeider. Følgelig er det vanskelig å avgjøre om vilkåret er tilstrekkelig konkretisert til å overholde de grunnleggende rettighetene som forordningen skal sikre.

Rapporten fra parlamentet i Østerrike viser videre at den tyske forbundsdagens parlamentariske grupper (Fraktionen) diskuterer en innføring av restriksjoner innen rammen av artikkel 23. Forslaget er å begrense rettigheten til innsyn og innhenting av kopi av møtereferatene til utvalgene for lukkede dører, retten til retting av personopplysninger i trykksaker og protokoller fra offentlige (plenums)møter og i publiserte uttalelser fra tredjeparter under offentlige høringer, og rett til transparent informasjon spesielt i forbindelse med undersøkelsesutvalg sin databehandling.

Særlig forslaget fra Tyskland kan inspirere avgrensningen ved en norsk bruk av artikkel 23. Utenriks- og forsvarskomiteen er en fast komité som behandler forslag om blant annet utenrikspolitiske forhold, militært forsvar og utviklingshjelp.⁵⁴ Majoriteten av sakene vil – gitt arten av komiteens saksmandat – angå særlig «national security» og «defence» jf. artikkel 23 nr. 1 bokstav (a) og (b).⁵⁵ Av denne grunn kan det være nærliggende med en løsning der GDPR sine bestemmelser er begrenset for hele komiteens arbeid på bakgrunn av artikkel 23. Dette vil i noen grad tilsvare forslaget til Tyskland om å begrense rettighetene til innsyn og innhenting av kopi av møtereferatene til utvalgene for lukkede dører.

De særskilte komiteene vil typisk også behandle saker knyttet til formålene nevnt i artikkel 23. Dette kan ses i lys av at både de særskilte komiteenes eksistens og de angitte formålene i artikkel 23 angår situasjoner som oppstår unntaksvis. Som eksempel kan arbeidet i de særskilte komiteene som ble oppnevnt i forbindelse med 22. juli-terroren og under koronapandemien knyttes til formålene «national security» og «public security» jf. artikkel 23 nr. 1 bokstav (a) og (c). Ettersom de særskilte komiteene oppnevnes for konkrete saker eller saker av bestemte slag⁵⁶, kan det være hensiktsmessig å åpne for at begrensningene gjennom artikkel 23 gjelder for de aktuelle komiteene i sin helhet dersom de øvrige vilkårene er innfridd. En forutsetning er at det også konkretiseres hvilken type rettighet som begrenses.

I hovedsak vil de fleste faste komiteene være underlagt GDPR. Det kan imidlertid ikke utelukkes at det oppstår enkeltsaker hvor anvendelsen av forordningens bestemmelser bør begrenses gjennom artikkel 23. En eventuell lovendring bør derfor også ta høyde for og sette rammer for vurderinger som må gjøres i den enkelte sak.

Det parlamentariske arbeidet omfatter mer enn komitéarbeid, og GDPR gjelder i utgangspunktet også for dette øvrige arbeidet – inkludert innsamling av personopplysninger via e-post og annen korrespondanse, samling og lagring. Også for dette mer generelle

⁵⁴ *Stortinget*, «Utenriks- og forsvarskomiteen»

⁵⁵ Det vises til drøftelsen av nasjonal sikkerhet under del 2 punkt 2.4.

⁵⁶ Jf. Stortingets forretningsorden § 18

parlamentariske arbeidet kan det tenkes tilfeller der en begrensning av GDPR sine bestemmelser bør finne sted. Rammeverket bør sørge for at den som er «controller» også har et verktøy å bruke i vurderingen av enkeltsaker.

Drøftelsen under dette punktet har søkt å illustrere konkrete tilfeller innen det parlamentariske arbeidet som er forankret i hensyn som gjør at det kan være behov for å begrense enkelte av de registrertes rettigheter etter GDPR gjennom nasjonal lovgivning. Potensiell lovgivning bør i så fall åpne for at begrensninger kan gjøres på bakgrunn av arbeidets art.

Jeg vil understreke at også andre formål angitt i artikkel 23 kan være relevante for å begrense anvendelsen av rettigheter og plikter etter GDPR på det parlamentariske arbeidet ved behandlingen av personopplysninger. Rammen for oppgavens omfang gjør at det ikke er anledning til å gjennomgå alle her.

4.4. Hvor kan begrensningen hjemles?

Personopplysningsloven gjennomfører GDPR i norsk rett. Derfor kan loven være et naturlig hjemmelsgrunnlag for eventuelle begrensninger av de registrertes rettigheter etter forordningen. Et alternativ er å innta et nytt kapittel i loven som regulerer forholdet til det parlamentariske arbeidet.

En forankring i personopplysningsloven vil oppfylle forutberegnelighetsaspektet ved lovskravet, forutsatt at formuleringen av begrensningen samsvarer med de øvrige kvalitative kravene som EU- og EMD-praksis oppstiller.

Reguleringen av forholdet mellom pliktene og rettighetene etter GDPR og det parlamentariske arbeidet kan hente inspirasjon fra andre lover. Sikkerhetsloven avgrenser sitt

virkeområde for Stortinget i § 1-4. Loven gjelder for Stortinget og Stortingets organer «så langt Stortinget bestemmer det». Lignende formulering er foreslått i den nye arkivloven.⁵⁷ Sikkerhetsloven gis dermed ikke direkte anvendelse for Stortingets parlamentariske virksomhet, og Stortinget må selv gjøre et formelt vedtak om spørsmålet.⁵⁸ Formuleringen gir likevel Stortinget en klar oppfordring til å fastsette bestemmelser på egenhånd. En tilsvarende formulering kan tenkes i en eventuell lovhjemmel som regulerer forholdet mellom GDPR og det parlamentariske arbeidet.

Selv om medlemslandet har ansvar for å nedfelle begrensningen i lovgivningen, innebærer ansvarlighetsprinsippet i artikkel 5 nr. 2 at det er «controller» som må dokumentere at GDPR er overholdt i det konkrete tilfellet.⁵⁹ Forutsatt at begrensningen er nedfelt i nasjonal lovgivning, har vedkommende ansvar for å vise at det er legitimt å bruke denne begrensningen i den aktuelle behandlingen av personopplysninger. Ansvarlighetsprinsippet krever at «controller» viser til årsakene for bruken av begrensningen hjemlet i artikkel 23, og tidspunktet og utfallet av nødvendighets- og proporsjonalitetsvurderingen⁶⁰. Prinsippet sikrer også at «controller» ikke gjør større unntak enn den nasjonale lovgivningen åpner for.

En eventuell lovendring bør derfor også gi den enkelte «controller» et verktøy for å sørge for at anvendelsen av begrensningen gjennom artikkel 23 er legitim i den konkrete saken, jf. artikkel 5 nr. 2.

Stortingets forretningsorden regulerer i stor grad hvordan stortingsrepresentantene skal gjennomføre sitt parlamentariske arbeid.⁶¹ Representantene har plikt til å innrette seg etter forretningsordenen jf. Grl. § 66 tredje setning, jf. Grl. § 80 annet ledd. Ettersom forretningsordenen allerede setter instruksjoner som representantene må overholde ved utøvelsen av det parlamentariske arbeidet, kan det være hensiktsmessig at den også adresserer hvordan

⁵⁷ Arkivlovutvalget (NOU 2019:9)

⁵⁸ Se Prop.153 L (2016-2017) punkt 19.1

⁵⁹ Hvm som er «controller» problematiseres under i punkt 5.2.

⁶⁰ EDPB Guidelines 10/2020 (2020), s. 5

⁶¹ Smith (2017), *Konstitusjonelt demokrati*. s. 194

kravene etter artikkel 5 nr. 2 kan etterleves der stortingsrepresentantene behandler personopplysninger i kraft av sitt virke.

Et alternativ er å innta en generell bestemmelse i Stortingets forretningsordenen som regulerer ansvaret for overholdelsen av GDPR, og som legger opp til at det kan gjøres endringer når det er behov som oppstår som er i tråd med unntaksbestemmelsen. Eksempelvis kan bestemmelsen angi arten av typen arbeid som kan aktualisere en begrensning i tråd med artikkel 23. Da vil en også kunne ta høyde for behandling av personopplysninger i eksempelvis *ad hoc*-situasjoner som oppnevningen av særskilte komiteer. Innlemmelsen vil bidra til at det ikke gjøres større unntak for det parlamentariske arbeidet enn det er lagt opp til på nasjonalt nivå gjennom personopplysningsloven.

Denne delen har utforsket hvordan artikkel 23 i praksis kan begrense anvendelsen av GDPR på deler av det parlamentariske arbeidet. Begrensningen må ha klar hjemmel i lov. Personopplysningsloven kan være et naturlig hjemmelsgrunnlag, da loven allerede gjennomfører GDPR i norsk rett og kan innfri vilkåret «legislative measure». En ytterligere regulering i Stortingets forretningsorden vil være et utfyllende supplement for å bidra til at den som er «controller» overholder ansvarlighetsprinsippet etter GDPR artikkel 5 nr. 2.

Likevel vil det oppstå andre praktiske utfordringer ved bruk av artikkel 23. Del IV vil gi overordnede bemerkninger til et utvalg av disse.

DEL IV: Avsluttende bemerkninger

1. Problemstillinger som bør avklares før en eventuell lovendring

1.1. «[C]ontroller» jf. artikkel 4 nr. 7

En begrensning gjennom artikkel 23 forutsetter at GDPR får anvendelse. Bruk av forordningen betinger imidlertid at de øvrige vilkårene i forordningen avklares med hensyn til det parlamentariske arbeidet. Avklaringen ligger utenfor rammene for oppgaven, men den følgende drøftelsen vil likevel skissere problemstillinger som en eventuell lovendring særlig må ta stilling til. Av hensyn til plass vil ikke det rettslige innholdet i vilkårene behandles inngående.

Vilkåret «controller» er definert i artikkel 4 nr. 7. Det må avklares om det er representantene selv eller for eksempel partigruppene eller komiteene som er «controller». I praksis er dette et spørsmål om hvem som har det overordnende ansvaret for at representantene overholder GDPR.

Dersom representantene anses som «controller» innebærer dette at de er personlig ansvarlig for behandlingen av personopplysningene. Rapporten innhentet av parlamentet i Østerrike viser at nederlandske Tweede Kamer der Staten-Generaal tolker vilkåret «controller» som en henvisning til parlamentarikerne selv.⁶² Det bærende argumentet deres er forskjellene mellom administrasjonen på den ene siden og parlamentsmedlemmene og de parlamentariske gruppene på den andre siden. Representantene anses derfor som individuelt ansvarlig som

⁶² ECPD, *REQUEST 4673* (2021) s. 3

«controller». I prinsippet vil tolkningen innebærer at hver enkelt representant må godtgjøre hvorfor unntaks- eller begrensningshjemmelen bør benyttes i det konkrete tilfellet. Det norske Stortinget består i dag av 169 stortingsrepresentanter. En praksis der hver enkelt representant vurderer behandlingen av personopplysninger vil fort kunne resultere i sprikende praktisering av GDPR, og dermed gi de registrerte et usikkert vern.

Et alternativ er at Stortingets administrasjon anses som «controller» etter artikkel 4 nr. 7. Administrasjonen bærer det overordnede ansvaret for IT-systemet, men har ikke tilgang til arbeidet som utføres av stortingsrepresentantene og dermed heller ikke hvilke personopplysninger de behandler. Dette innebærer at administrasjonen ikke vil kunne utføre de plikter som påhviler en «controller» etter GDPR. Mangel på informasjon om hvilke personopplysninger stortingsrepresentantene behandler vil blant annet avskjære administrasjonen fra å gi de registrerte informasjon om hvilke personopplysninger som behandles, hvor lenge de lagres og hvem som har tilgang til disse jf. artikkel 5, 12, 13 og 14. En konstellasjon der administrasjonen er «controller» på vegne av stortingsrepresentantene er heller ikke forenlig med at administrasjonen hverken har kontroll- eller styringsrett overfor representantene, blant annet fordi GDPR artikkel 28 nr. 3 da vil kunne innebære et avtaleforhold hvor representantene er underlagt administrasjonen.

1.2. «[S]upervisory authority» jf. artikkel 51 jf. artikkel 4 nr. 21

Forordningen har et eget kapittel som regulerer oppnevningen av tilsynsorgan og tilhørende oppgaver i kapittel VI. Etter GDPR artikkel 51 skal medlemsstatene «provide for one or more independent public authorities» for «monitoring the application of this Regulation [...]». Organet blir omtalt som «supervisory authority» og er nærmere definert i artikkel 4 nr. 21. I Norge er Datatilsynet utnevnt som «supervisory authority».

Tilsynsorganets oppgaver er nedfelt i GDPR artikkel 57 og innebærer i Norge at Datatilsynet blant annet har mandat til å «monitor and enforce the application of this Regulation» jf.

bokstav (a) og «conduct investigations on the application of this Regulation [...]» jf. bokstav (h).

Storingsrepresentantene er folkevalgte og uavhengige ombudspersoner. Premisset fremgår av Grunnloven og er en forutsetning for demokratiet. Følgelig vil en kontrollfunksjon der Datatilsynet har myndighet til å «monitor and enforce the applicaiton of this Regulation [...]» jf. GDPR artikkel 57 bokstav (a) overfor stortingsrepresentantene kunne komme i konflikt med Grunnlovens forutsetninger og representantenes rolle som uavhengige ombudspersoner.

Relasjonen mellom Datatilsynets mandat som tilsynsorgan etter artikkel 51 og parlamentariskenes uavhengige rolle tilsier at en alternativ løsning bør vurderes.

Rapporten innhentet av parlamentet i Østerrike viser at de fleste landene i Europa anser det parlamentariske arbeidet som underlagt nasjonale tilsynsorgans myndighet. Ingen av landene har opprettet eget tilsynsorgan for behandling av personopplysninger i det parlamentariske arbeidet.

Tyskland har flere etablerte tilsynsorgan, og kompetansen overfor det parlamentariske arbeidet ligger hos the Federal Commissioner for Data Protection and Freedom and Information.

I 8 av parlamentene, herunder blant annet Østerrike, Kypros og Finland, er behandlingen av personopplysninger i det parlamentariske arbeidet derimot ikke underlagt «a supervisory authority's remit». Hovedargumentet oppgis å være maktfordelingsbetraktninger.⁶³ Tilnærmingen innebærer at behandlingen av personopplysninger i det parlamentariske arbeidet ikke er underlagt reell kontroll. EU-domstolens reaksjon på nettopp manglende

⁶³ Se König (2022) s. 7

kontroll – riktignok domstolskontroll – i *Schrems II [GC]*, C-311/18⁶⁴, kan tilsi at behandling av personopplysninger som ikke er underlagt et reelt tilsynsorgan vil være problematisk etter forordningen. Det er imidlertid interessant å merke seg at enkelte av disse landene – blant annet Østerrike og Finland – mener at det parlamentariske arbeidet ikke reguleres av forordningen, jf. artikkel 2 nr. 2. Det er dermed noe underlig at de likevel har tatt stilling til spørsmålet om betydningen av «supervisory authority» i forordningen. Dette er et ytterligere argument for at problemstillingen bør avklares på europeisk nivå, ettersom det vitner om at rekkevidden av tilsynsmyndighetens mandat er uklar.

Rapporten viser også at enkelte parlamenter ikke har tatt stilling til spørsmålet enda. Blant annet vurderer Estland det nasjonale estiske databeskyttelsesinspektoratet som tilsynsorgan, og fremhever muligheten for å avklare spørsmålet i domstolene – men foreløpig har ingen saker blitt fremsatt. Irland har til en viss grad vurdert å opprette en separat tilsynsmyndighet for det parlamentariske arbeidet. Likevel trekker de frem at artikkel 51 – om tilsynsorganets myndighet – ikke i tilstrekkelig grad respekterer maktfordelingen, fordi de registrerte har adgang til å rette klage mot tilsynsorganet etter artikkel 78.

Blant land som ikke har adressert forholdet mellom tilsynsmyndigheten sin kompetanse og det parlamentariske arbeidet, inngår også Norge. I forbindelse med utformingen av personopplysningsloven ga Datatilsynet, som er Norges tilsynsorgan, uttalelser i forarbeidene der de selv adresserer behovet for avklaringer. Med hensyn til virkeområde viser de til at «det kan være viktig å vite hvor grensen går mellom tilfeller der man er EØS-rettslig forpliktet til å følge forordningen og der man ikke har en slik forpliktelse» og at dette «vil ha betydning på et område hvor forordningen krever eller gir adgang til nærmere nasjonal regulering». Datatilsynet uttaler på denne bakgrunn at «det bør utarbeides en veiledning om grensedragningen, enten i utredningsinstruksen eller på annet vis».⁶⁵

⁶⁴ Se særlig avsnittene 192 og 196 flg. der poenget var sentralt for underkjenningen av *Privacy Shield* som overføringsgrunnlag for personopplysninger til USA som tredjeland.

⁶⁵ Prop. 56 L (2017-2018) punkt 4.4.1.

2. Behov for avklaring på europeisk nivå

En eventuell begrensning etter artikkel 23 må gjennomføres av lovgiver. Ettersom det er Stortinget som vedtar lover, vil representantene – dersom de anses som «controller» – i realiteten være med på å vedta begrensningene. Dette kan komme i konflikt med at ansvaret påhviler den aktuelle «Member State» og ikke den enkelte «controller» etter artikkel 23. Utfordringene som oppstår grunnet Stortingets rolle som lovgiver er et argument for at avklaringen av forholdet mellom GDPR og det parlamentariske arbeidet ikke bør ligge nasjonalt, men overnasjonalt. Kommisjonen og Rådet i EU, eventuelt EDPB, bør ta stilling til spørsmålet.

Et ytterligere poeng, også nevnt innledningsvis, er at rapporten innhentet av Østerrike gir indikasjoner på at det er et behov for å harmonisere tolkningen og håndhevelsen av GDPR for det parlamentariske arbeidet i Europa. Det er problematisk at de ulike europeiske parlamentene har en sprikende tilnærming til spørsmålet om GDPR og det parlamentariske arbeidet. Formålet med å gå vekk fra direktiv og over til forordningen var nettopp for å sørge for et likt vern for de registrerte på tvers av landegrensene. Den manglende adressering av denne grunnleggende problemstillingen kan sies å undergrave deler av formålet med å innføre forordningen. Også dette tjener som argument for at EU bør ta uttrykkelig stilling til anvendelsen av GDPR på det parlamentariske arbeidet.

Gjennom denne masteroppgaven har jeg søkt å kartlegge hvilke rettslige alternativer som foreligger etter gjeldende rett og gi min tolkning på hva som kan være en hensiktsmessig løsning – som både overholder de registrertes rett til vern om personopplysninger og som samtidig tar høyde for de konstitusjonelle og praktiske aspektene ved det parlamentariske arbeidet. Skisseringen av alternativer har vært rettet mot norske lovgivere. Men ettersom det parlamentariske arbeidet har sterke nasjonale forankringer, og dette gir opphav til ulik tolkning av den felleseuropeiske forordningen, bør den overordnede harmoniseringsprosessen løses på EU-nivå for å sikre etterlevelse av unionens formål om et ensrettet vern om personopplysninger.

3. Konklusjon

Konklusjonen er at GDPR kommer til anvendelse for det parlamentariske arbeidet, jf. artikkel 2. Gjennom artikkel 23 åpnes det likevel for en *delvis* anvendelse av GDPR på det parlamentariske arbeidet, gitt at lovgiver nedfeller begrensningen i tråd med bestemmelsens vilkår.

Litteraturliste

NORSKE (RETTS)KILDER

Lovgivning

Grunnloven

Lov 17. mai 1814 om Kongeriket Norges Grunnlov

EØS-loven

Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) mv. (EØS-loven)

Personopplysningsloven – opphevet

Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) *Opphevet*

Sikkerhetsloven

Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)

Personopplysningsloven

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

Lovforarbeider og offentlige utredninger

Innst. 207 S (2011-2012)

Innst. 207 S (2011-2012) Innstilling fra Den særskilte komité om redegjørelse fra justisministeren og forsvarsministeren i Stortingets møte 10. november 2011 om angrepene 22. juli

Prop.153 L (2016-2017)

Prop.153 L (2016-2017) Lov om nasjonal sikkerhet (sikkerhetsloven)

Prop.56 LS (2017-2018)

Prop.56 LS (2017-2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen

om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordningen) i EØS-avtalen

Arkivlovutvalget (NOU 2019:9)

Arkivlovutvalget (NOU 2019:9) Fra kalveskinn til datasjø. Kapittel 1, Innledende bestemmelser

Praksis fra underinstanser, reglementer og uttalelser fra andre norske institusjoner

Stortingets forretningsorden

7. juni 2012, Stortingets forretningsorden. Regler for saksbehandlingen i Stortinget.
FOR-2012-06-07-518

Nasjonal sikkerhetsmyndighet, Figur 3.2.

Nasjonal sikkerhetsmyndighet, *Veilder i departementenes identifisering av grunnleggende nasjonale funksjoner*, "Figur 3.2: Nasjonale sikkerhetsinteresser, underkategorier og utdyping av disse". Lest 25. april 2022.

<https://nsm.no/nasjonale-sikkerhetsinteresser/category1193.html>

Stortinget. Referat fra stortingsmøte 16. mars 2020

Stortinget. Referat fra stortingsmøte 16. mars 2020.

<https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2019-2020/refs-201920-03-16?all=true>

PVN-2020-19

Den norske personvernemnda. Personvernemndas vedtak 2. februar 2021. PVN-2020-19.

Referat, Stortingets sikkerhetsstab (2022)

Referat - møte med Stortingets sikkerhetsstab. 7. mars 2022, Stortinget, Oslo.
(vedlegg nr. 2)

Juridisk og øvrig litteratur

Fredriksen og Mathisen (2018), *EØS-rett*

Fredriksen, Halvard Haukeland og Mathisen, Gjermund, *EØS-rett*, 3. utgave, Fagbokforlaget, 2018

Grimstad (2021), *Stortingets forretningsorden med kommentarer*

Grimstad, Kyrre, *Stortingets forretningsorden med kommentarer*, oktober 2021, Stortinget

Schartum (2020), *Personvernforordningen*

Schartum, Dag Wiese, *Personvernforordningen – en lærebok*, 1. utg., Fagbokforlaget 2020.

Smith (2017), *Konstitusjonelt demokrati*

Smith, Eivind, *Konstitusjonelt demokrati: statsforfatningsretten i prinsipielt og komparativt lys*, 4. utgave, Fagbokforlaget, 2017

Digitale kilder

Olsen, (note a5-1)

Olsen, Thomas, *Norsk Lovkommentar*, note (a5-1). Rettsdata.no

Olsen, (Art. 85 1-2)

Olsen, Thomas, *Norsk Lovkommentar* (Art. 85 1-2). Rettsdata.no

Orgeret (2020)

Orgeret, Kristin Skare, "Fjerde statsmakt" Store norske leksikon, 3. juni 2020, https://snl.no/fjerde_statsmakt (lest 13. april 2022).

Stortinget, "Fagkomiteene"

Stortinget, "Fagkomiteene", sist oppdatert 14.01.2022, <https://www.stortinget.no/no/Stortinget-og-demokratiet/Organene/Komiteene/>

Stortinget, "Hva gjør en representant?"

Stortinget, "Hva gjør en representant?", <https://www.stortinget.no/no/Stortinget-og-demokratiet/Representantene/Hva-gjor-en-representant/> sist oppdatert 23.03.2017

Stortinget, "Komitéarbeidet"

Stortinget, "Komitéarbeidet", <https://www.stortinget.no/no/Stortinget-og-demokratiet/Arbeidet/Saksbehandlingen-i-komiteene/> sist oppdatert 03.01.2022

Stortinget, "Utenriks- og forsvarskomiteen",
Stortinget, "Utenriks- og forsvarskomiteen",
<https://www.stortinget.no/no/Representanter-og-komiteer/Komiteene/Utenriks--og-forsvarskomiteen/>

Trondal (2019)

Trondal, Jarle, "EUs fire friheter" Store norske leksikon, 16. mai 2019,
https://snl.no/EUs_fire_friheter (lest 25. april 2022)

INTERNASJONALE (RETTS)KILDER

Lovgivning og traktater

Den europeiske menneskerettighetskonvensjonen (EMK)

Europarådet, Den europeiske menneskerettighetskonvensjonen (EMK), 4. november 1950

Direktiv 95/46/EF (95-direktivet)

Europaparlamentet og Rådets direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. *Opphevet*

Den europeiske unions pakt om grunnleggende rettigheter (Charteret)

Den europeiske unions pakt om grunnleggende rettigheter («Charteret»), 2012/C 326/02

Traktaten om Den europeiske union (TEU)

Konsolidert versjon av Traktaten om Den europeiske union, TEU, OJ 2016/C 202/1 s. 13

Traktaten om Den europeiske unions virkemåte (TEUV)

Konsolidert versjon av Traktaten om Den europeiske unions virkemåte, TEUV, OJ 2016/C 202/1 s. 47

Personvernforordningen (GDPR)

Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri

utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (GDPR)

Rettsavgjørelser fra EU-domstolen og EMD

Nilsson and others [C5] C-162/97

Dom av 19. november 1998 [C5], *Nilsson and others*, C-162/97, EU:C:1998:199

Satakunnan Markkinapörssi and Satamedia [GC], C-73/07

Dom av 16. desember 2008 [GC], *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727

Digital Rights Ireland Ltd [GC], C-594/12

Dom av 8. april 2014 [GC], *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*, C-594/12, EU:C:2014:238

Buivids [C2], C-345/17

Dom av 14. februar 2019 [C2], *Buivids*, C-345/17, EU:C:2019:122

Land Hessen [C3], C-272/19

Dom av 9. juli 2020 [C3] *VQ v Land Hessen*, C-272/19, EU:C:2020:535

Schrems II [GC], C-311/18

Dom av 16. juli 2020 [GC], *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II")*, C-311/18, EU:C:2020:559

Latvijas Republikas Saeima [GC], C-439/19

Dom av 22. juni 2021 [GC], *Latvijas Republikas Saeima (Points de pénalité)*, C-439/19, EU:C:2020:1054

Malone mot Storbritannia [1984]

Malone mot Storbritannia 1984, no. 8691/79, ECHR 10

Magyar Helsinki Bizottság mot Ungarn, [2016]

Magyar Helsinki Bizottság mot Ungarn, 2016, ECHR:2016:1108JUD001803011

Summary of the Request for a Preliminary Ruling, C-33/22

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice, C-33/22, Österreichische Datenschutzbehörde.

Working Document. 14. januar 2022.

Oversættelsen fra CJEU (henvist til i teksten):

[https://curia.europa.eu/juris/showPdf.jsf?docid=257122&pageIndex=0&doclang=EN
&mode=lst&dir=&occ=first&part=1&cid=3558177](https://curia.europa.eu/juris/showPdf.jsf?docid=257122&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3558177)

Original (på tysk):

https://www.vwgh.gv.at/rechtsprechung/vorabentscheidungsantraege_an_den_eugh/EU_2021_0009.pdf?8hkygt

Utredninger, retningslinjer, rapporter og andre kilder

Danske justitsministeriet (nr. 1565)

Danske justitsministeriet, *Betænkning om Databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning*, Del I, bind 2., Betænkning nr. 1565.

https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/betaenkning_nr_1565_del_i_bind_2.pdf

Den Danske Ordbog, "herunder"

Den Danske Ordbog, "herunder", <https://ordnet.dk/ddo/ordbog?query=herunder>

EDPB, *Guidelines 10/2020* (2020)

Det europæiske personvernrådet, *EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR*. Version 1.0. 15. desember 2020.

https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf

ECPRD, *REQUEST 4673* (2021)

The European Centre for Parliamentary Research and Documentation (ECPRD), *ECPRD-REQUEST 4673 Concerning the GDPR'S Application in Parliamentary Core Areas Final Summary*, Juli 2021
(vedlegg nr. 1)

König (2022)

König, Sarah, *The GDPR's Application and Supervisory Authorities' Remit on National Parliaments' Data Processing in Parliamentary Core Activities*, International Journal of Parliamentary Studies (2022) 1-11, Brill
(vedlegg nr. 4)

Posnik (2021)

Posnik, Rosi, *Legal Considerations on the CJEU Judgement of 9 July 2020, C-272/19*, International Journal of Parliamentary Studies (2021) 154-159, Brill
(vedlegg nr. 3)

VEDLEGG

1. ECPRD, *REQUEST 4673* (2021)



REPUBLIC OF AUSTRIA
Parliament

ECPRD-REQUEST 4673

CONCERNING

THE GDPR'S APPLICATION IN PARLIAMENTARY CORE AREAS
FINAL SUMMARY

July 2021

Sarah König, DPO Austrian Parliamentary Administration
e-mail: sarah.koenig@parlament.gv.at

Dr. Christoph Konrath, ECPRD Correspondent
e-mail: christoph.konrath@parlament.gv.at



INTRODUCTION

Since the General Data Protection Regulation's (GDPR)¹ entry into force in 2018, the question whether its material scope of application is extended to data processing in parliamentary core areas has been debated widely and answered differently by ECPRD's members. The European Court of Justice's (CJEU) decision *Land Hessen* of 9 July 2020, C-272/19, determining a petition's committee of the German regional Parliament of *Land Hessen* as controller within the meaning of the GDPR and thus subjecting this committee's processing of personal data to the GDPR's applicability, has sparked the debate anew. The ECPRD-Request 4673 sought to provide ECPRD's members with an update to similar previous requests (especially 3890). Questions asked were:

1. Does your parliament hold the view that the processing of personal data in core areas of the national parliament (i.e. committee and plenary proceedings, committee reports, stenographic records, interpellations, committees of inquiry) is subject to the GDPR or that exceptions as stipulated in Art. 2 GDPR apply?

1a. If the answer is "yes": Are there national regulations that delineate the material scope of the GDPR in more detail with regard to core areas of parliamentary activities (i.e. exceptions)? Can you describe those regulations and reference them?

1b. If the answer is "no": Are there national regulations on data protection with regard to core areas of parliamentary activities? Can you describe those regulations and reference them?

2. Do you plan or discuss to amend data protection regulations and practices in core areas of parliamentary activities? If so, can you describe them briefly?

3. Can a person whose personal data has been processed in core areas of parliamentary activities (i.e. in an interpellation) bring the matter to the attention of an independent oversight body? If yes, is this a special oversight body only for matters regarding parliament? Can you describe the relevant regulations and reference them?

A total of 33 parliamentary chambers replied². In the following, their answers are summarized and clustered where possible.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² Austria (2), Belgium (2), Bulgaria, Croatia, Cyprus, Czech Republic (2), Denmark*, Estonia, Finland, France, Germany (2), Greece*, Hungary, Ireland (2), Italy (2), Latvia, Lithuania, Malta*, Netherlands (2), Poland – Sejm, Portugal, Romania – Senat, Slovakia, Slovenia – National Assembly, Spain – Congreso de los Diputados, Sweden. *Denmark's, Greece's and Malta's positions were issued individually at a later stage. The parliament of Luxembourg, Poland's Senat, the Romanian Camera Deputatilor, the Slovene National Council and Spain's Senat did not reply, Norway's Stortinget and the French Senate did not reply content wise.



SUMMARY

1. A majority of parliamentary chambers (22 of 33; 66,67 %) considers the GDPR to be applicable on data processing in parliamentary core activities opposing 7 (21,21 %) parliamentary chambers who refer to the exemption of Art. 2 para 2 subpara a GDPR in this context.

- 22 parliamentary chambers consider core parliamentary activities to fall within the GDPR's material scope of application, albeit 7 of them indicate (the possibility of) an indirect application of the GDPR brought about by national stipulations. The second group includes both Belgian chambers³, the German Bundestag⁴, Greece, the Italian Camera Dei Deputati⁵, Slovenia's National Assembly⁶ and Sweden's Riksdag⁷. However, the German Bundestag and the Swedish Riksdag have not yet settled on a final position in this matter. [For further information, please see answers to 1a.]
- 7 parliamentary chambers deem the exemption of Art. 2 para 2 subpara a GDPR applicable and thus deny the GDPR's applicability on core parliamentary activities. These are the parliaments of Austria (both chambers), Denmark, Finland, Malta and Ireland (both chambers). [For further information, please see answers to 1b.]
- The remaining 4 parliaments/chambers (Croatia, Cyprus, Italy's Senate, and Romanian Senat) did not substantially elaborate or settle on a final position.

1. a. Parliaments that apply the GDPR could make use of "opening clauses" and thus deviate from or specify certain provisions of the GDPR, e.g. legally determine the role of the "controller", restrict rights and obligations, as well as determine lawful data processing. Of the 22 parliamentary chambers that apply the GDPR (at least indirectly), only 3 have not listed national data protection regulations that complement the GDPR when processing personal data in parliamentary core activities.

- No relevant national legislation was cited by the parliament of Bulgaria, France's Assemblée Nationale and the German Bundesrat. In Portugal, the President of the Assembly of the Republic has issued the Order n.º 88/XIII with regard to the GDPR and the processing of personal data by Parliament, which, however, does not include any exemptions from the GDPR's regime.
- Concerning the stipulation of a "controller" (Art. 4 para 7 GDPR), the Dutch Tweede Kamer der Staten-Generaal highlights its distinction from Members of Parliament and parliamentary groups who are

³ [Art. 2 Framework Data Protection Law](#) extends the GDPR's scope of application, notably in cases of Art. 2 para 2 subpara a and b GDPR [Link in French].

⁴ The GDPR is applied indirectly by means of a national regulation also in core parliamentary activities (committee and plenary proceedings, stenographic records, etc.).

⁵ The national legislation on data protection (DECRETO LEGISLATIVO 10 August 2018, n. 101) extends the application of Art. 9 and 10 GDPR to data processing in parliamentary core activities.

⁶ Data processing is based on the national [Personal Data Protection Act](#) and [Art. 21 to 24 National Assembly Act](#) [Links in Slovene].

⁷ Chapter 1 Section 2 of [Act \(2018:218\) on Supplementary Provisions to the General Data Protection Regulation](#) extends the application of the GDPR outside the material scope of the GDPR [Link in English].



individually responsible as "controllers". Also in the [Czech Republic](#), Deputies are considered to be "controllers" when acquiring personal data in the exercise of their mandate.

- Stipulations of lawful data processing in parliamentary core areas (Art. 6 para 1 subpara c or e in conjunction with para 3 GDPR, Art. 9 para 2 subpara g GDPR) were referenced by [Cyprus](#) (Section 5(b) of the national [Data Protection Law](#)) and especially [Hungary](#) whose Act on the National Assembly contains detailed provisions e.g. on data processing when justifying a Member's absence and other (administrative) data processing carried out by the Office of the National Assembly that – among other information (such as data types, storage periods) and in accordance with the requirements of Art. 6 para 3 GDPR – *list the purposes of the respective processing*. [Italy's](#) national Data Protection Law defines the reasons of substantial public interest (within the meaning of Art. 9 para 2 subpara g GDPR) that authorise the processing of special types of personal data, several of which apply to parliamentary activities, as well.
- On restrictions of rights and obligations (Art. 23 GDPR) and other "opening clauses":
 - Following the CJEU's decision *Land Hessen*, the [German Bundestag's](#) parliamentary groups (Fraktionen) are currently discussing the introduction of restrictions within the scope of Art. 23 GDPR. [See answers to 2. for further information.] In [Italy](#), national legislation on data protection already restricts data subjects' rights in the context of data processing by an inquiry commission (i.e. effectively using Art. 23 GDPR).
 - [Estonia](#) plans to make use of exceptions provided for in the GDPR, expressly Art. 85 and 86 after altering its position (see ECPRD-request # 3890) following the CJEU's decision *Land Hessen* to now considering the GDPR (and also the national [Personal Data Protection Act](#)) applicable in parliamentary core areas.

1. b. Parliaments that deny the (even indirect) application of the GDPR in core parliamentary activities rely on national (constitutional) provisions when processing personal data.

- [Austria's parliament](#) and the [Irish Houses of the Oireachtas](#) both abide by good data protection practice given both their constitutions grant a fundamental right to privacy that also applies in parliamentary core activities' data processing⁸. However, one difference is that in [Ireland](#), [Section 60 \(1\)\(a\) and \(3\)\(a\)\(i\) of the Data Protection Act 2018](#) stipulates a general restriction to rights and obligations of the GDPR rendering effective the opening clause Art. 23 GDPR to safeguard – amongst others – [parliamentary privilege](#).
- [Finland](#) expressly exempts also the national Data Protection Act's application when parliamentary activities are concerned ([Section 2 para 2 Data Protection Act](#))⁹; still Parliament's Rules of Procedure contain regulations on the publicity/confidentiality of committee documents and explicitly deem personal data concerning financial status or health as confidential unless compelling public interest requires their publication ([Section 43a para 1 and 2 Rules of Procedure](#)).

⁸ For Austria, please see For Austria, please see [§ 1 Federal Act concerning the Protection of Personal Data \(DSG\)](#).

⁹ As does Austria, except § 1 DSG.



2. No parliament indicated concrete plans for legislative amendments. The Estonian Riigikogu and the German Bundestag are amidst discussions to make use of opening clauses; other parliaments are referring to administrative projects.

- Use of opening clauses: [Estonia's Riigikogu](#) indicates plans for using exemptions in the context of Art. 85 and 86 GDPR; the [German Bundestag's](#) parliamentary groups (*Fraktionen*) discuss if use of Art. 23 GDPR's restrictions to obligations and rights should be made (i.e. restrictions to the rights to access and obtaining a copy of in camera committee sittings' minutes, the right to rectification of personal data in printed matters and records of public (plenary) meetings as well as in published statements made by third parties during public hearings, the right to transparent information especially in the context of inquiry committees' data processing).
- The [Belgian](#) national Framework Data Protection Law is currently undergoing comprehensive evaluation; the [Danish Folketinget](#) is considering possible partial applicability of the GDPR, the [Hungarian parliament](#) references an internal strategy that seeks to strengthen the data protection framework (including assessments of data management, guidance, impact and the coordinating, advisory and control role of the DPO); similarly, [Italy's Senate](#) mentions ongoing efforts to render procedures effective (a working group has been established).
- The [German Bundesrat](#) reports on political efforts to exclude the Federal States' Parliaments from the GDPR's scope of application.

3. No parliament reported a special oversight body for data processing in the context of parliamentary core activities. In most cases, the national supervisory authority is the competent oversight body.

- 20 (60,61 %) parliamentary chambers' data processing in core parliamentary areas is subject to the respective national supervisory authority's remit. In [Germany](#), where more than one such supervisory authority is established, the competence lies with the Federal Commissioner for Data Protection and Freedom of Information.
- The data processing in parliamentary core areas of 8 parliamentary chambers (24,24 %), namely, [Austria \(both chambers\)](#), [Cyprus](#), [Denmark](#), [Finland](#), [Italy \(both chambers\)](#) and [Malta](#), is not subjected to a supervisory authority's remit. The main reason for this seem to be strict concepts of the separation of powers and parliamentary autonomy.
- 3 parliamentary chambers are still undecided on this matter: The [Estonian Riigikogu](#) tends to see a possible remit of the national Estonian Data Protection Inspectorate, but highlights the definite option of a court settlement (so far no cases have been brought forward). [Ireland's Houses of the Oireachtas](#) is in exchange with the national Data Protection Commission but tends to be of the opinion that the only recourse a data subject has, is to an appropriate Committee of each House as contemplated by that House's Standing Orders (these might constitute as special supervisory bodies). The establishment of a discrete (i.e. separate) parliamentary supervisory authority, however, is met with scepticism as Art. 51 GDPR would not sufficiently respect the separation of powers given the imperative provision for a judicial remedy in Art. 78 GDPR.



COMPREHENSIVE OVERVIEW

Parliamentary chamber	GDPR application	Planned amendments	Supervisory body
Austria (National Council, Federal Council)	N	N	N
Belgium (Chambre des Représentants, Sénat)	Y	(Y)	Y
Bulgaria – National Assembly	Y	N	Y
Croatia – Hrvatski Sabor	undefined ¹⁰	N	Y
Cyprus – House of Representatives	undefined	N	N
Czech Republic (Chamber of Deputies, Senat)	Y	N	Y
Denmark – Folketinget	N	Y	N
Estonia – Riigikogu	Y	undecided	undecided
Finland – Eduskunta	N	N	N
France – Assemblée Nationale	Y	N	Y
France – Sénat	N/A		
Germany – Bundesrat	Y	N	Y
Germany – Bundestag	(Y)	Y	Y
Greece – Vouli tôn Ellínōn	Y	(Y) ¹¹	Y
Hungary – National Assembly	Y	Y	Y
Ireland (Houses of the Oireachtas)	N	N	undecided
Italy – Camera Dei Deputati	Y	N	N
Italy – Senato della Repubblica	undefined ¹²	Y	N
Latvia – Saeima	Y	N	Y
Lithuania – Seimas	Y	N	Y
Luxembourg – Chambre des Députés	N/A		
Malta – House of Representatives	N	N	N

¹⁰ GDPR is applied to affairs of public administration (i.a. complaints and petition process, publication of MPs questions to government).

¹¹ Amendments to the Standing Orders were considered possible during the presentation at the ECPRD's Webinar on Parliaments and the GDPR on June, 14th 2021.

¹² However, the situation could be updated in the near future, switching to "Y".



Parliamentary chamber	GDPR application	Planned amendments	Supervisory body
Netherlands – Eerste Kamer der Staten-Generaal, Tweede Kamer der Staten-Generaal	Y	N	Y
Norway – Stortinget	N/A		
Poland – Sejm	Y	N	Y
Poland – Senat	N/A		
Portugal – Assembleia da Republica	Y	N	Y
Romania – Camera Deputatilor	N/A		
Romania – Senat	undefined	N	undefined
Slovakia – National Council	Y	N	Y
Slovenia – National Council	N/A		
Slovenia – National Assembly	Y	N	Y
Spain – Congreso de los Diputados	Y	N	undefined
Spain – Senat	N/A		
Sweden – Riksdag	(Y)	N	Y

Table 1: Overview of parliamentary chambers' material application of the GDPR in parliamentary core areas, planned amendments and established oversight in this context.

2. Referat – møte med Stortingets sikkerhetsstab

REFERAT – MØTE MED STORTINGETS SIKKERHETSSTAB

Referat

Dato: 7. mars 2022

Sted: Stortinget

Til stede: Stortingets sikkerhetsstab, Stortingets personvernombud og kandidaten

Parlamentarisk arbeid som angår nasjonal sikkerhet

Vi diskuterte særlig bestemmelsen i GDPR artikkel 2 nr. 2 (a), som avgrenser forordningens virkeområde mot behandling av personopplysninger som skjer «outside the scope of Union law». Rettskildene tilsier at vilkåret unntar nasjonal sikkerhet fra GDPR sitt anvendelsesområde.

Hensikten med møtet var å få et praktisk innblikk i hvilke deler av det parlamentariske arbeidet som typisk angår nasjonal sikkerhet.

Basert på sikkerhetsstabens redegjørelse, er det samlet sett ikke veldig mye av det «daglige» parlamentariske arbeidet som knyttes til nasjonal sikkerhet. Det enkelte komiteer som behandler informasjon av nasjonal sikkerhet, eksempelvis utenriks- og forsvarskomiteen og kontroll- og konstitusjonskomiteen. Kommisjoner blir utnevnt ut fra behov, og et forslag som ble luftet var at en i utnevnelsen kan ta stilling til GDPR sin eventuelle anvendelse basert på den informasjonen som skal behandles.

I den grad arbeidet angår nasjonal sikkerhet, faller dette under sikkerhetsloven. Gruppene regnes som juridiske enheter.

For spørsmålet om en eventuell regulering av det parlamentariske arbeidets forhold til GDPR, ble det foreslått at man kan hente inspirasjon fra formuleringene i sikkerhetsloven. Loven har en egen bestemmelse om anvendelse for Stortinget. Bestemmelsen i § 1-4 angir at loven gjelder for Stortinget og Stortingets organer «så langt Stortinget bestemmer det».

3. Rosi Posnik (2021)



BRILL

INTERNATIONAL JOURNAL OF PARLIAMENTARY STUDIES
1 (2021) 154-159

INTERNATIONAL
JOURNAL OF
PARLIAMENTARY
STUDIES

Legal Considerations on the CJEU Judgement of 9 July 2020, C-272/19

Rosi Posnik

Legal, Legislative and Research Services, Austrian Parliamentary
Administration, Vienna, Austria
rosi.posnik@parlament.gv.at

Abstract

In a preliminary ruling procedure initiated by the Administrative Court of Wiesbaden (Germany), the CJEU ruled that the processing of personal data carried out by the Petitions Committee of the Parliament of *Land* Hessen is subject to the GDPR in so far as the Committee determines, alone or with others, the purposes and means of the processing, and thus it must be categorised as a ‘controller’, within the meaning of the GDPR. This article takes a critical look at the legal arguments of the CJEU.

Keywords

data protection – GDPR – parliament – Petitions Committee

General

The proceedings arose against the following background:

A person who had submitted a petition to the Petitions Committee of the Parliament of *Land* Hessen applied to that committee, on the basis of Article 15 GDPR, for access to his personal data, which had been logged by that committee when dealing with his petition. The President of the Parliament of *Land* Hessen rejected that application, on the grounds that the petition procedure constitutes a function of parliament and that parliamentary business was outside the scope of the GDPR. The applicant therefore brought an action before the Administrative Court of Wiesbaden.

The Administrative Court noted that German law grants no right of access to personal data processed in the context of a parliamentary petition. With its request for a preliminary ruling, it asked the Court whether the GDPR, in particular Article 15, is applicable to the committee of a Federated State's parliament that is responsible for dealing with the petitions of citizens and whether such a body would constitute an authority within the meaning of Article 4(7) GDPR.

Reasoning of the CJEU

The CJEU ruled that the Petitions Committee of the Parliament of *Land Hessen*, in so far as this committee places conditions, alone or with others, on the purposes and means of the processing of personal data, must be categorised as a 'controller' within the meaning of the GDPR and that the processing of personal data carried out by such a committee is subject to the GDPR.

The CJEU justified its decision by referring to the fact that the activities of the Petitions Committee do not fall under one of the exceptions provided for in the GDPR concerning its material scope of application. In its decision, the Court listed four points:

- 1) The definition of 'controller' (Article 4(7) GDPR) is not limited to authorities, but is sufficiently wide to include any body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- 2) In response to the argument of *Land Hessen's* Parliament that the activities of a parliamentary committee fall outside the scope of EU law within the meaning of Article 2(2) GDPR, the CJEU referred to its judgement of 6 November 2003, *Lindqvist*, C-101/01, regarding Article 3(2) of the Data Protection Directive 95/46/EC. In this judgement, the Court stated that although the Directive was based on Article 100a of the EC Treaty (now Article 95 TEU), the recourse to that legal basis does not presuppose the existence of an actual link to the free movement between Member States in every situation. It would be inappropriate to interpret the expression 'activity which falls outside the scope of Union law' as stipulating a requirement to review, case-by-case, each specific measure's potential to directly affect the free movement between Member States.

According to the CJEU, this applies even more to the GDPR, which is based on Article 16 TFEU – provisions relating to the protection of individuals with regard to the processing of personal data in the course of activities that fall within the scope of EU law, and to the free movement of such data – and whose Article 2(2) essentially corresponds to Article 3(2) of the Directive 95/46/EC.

- 3) Article 2(2)(a) GDPR (exception for activities which fall outside the scope of Union law) must be interpreted restrictively, as it constitutes an exception to the very wide material scope of Article 2(1) GDPR. The CJEU again referred to the *Lindqvist* judgement and concluded that for this exception to apply, it is not sufficient that an activity is one which is characteristic of the State or the public authority concerned. It is necessary that the activity is one of those explicitly mentioned in the exceptions (of Article 2 GDPR) or that it can be classified in the same category as those activities – this was denied by the CJEU in the specific case. The Court held that the activities of the Petitions Committee of the Parliament of *Land Hessen* are incontestably public and characteristic of that Federated State, since the committee indirectly contributes to the parliamentary activity, but it considered these activities also to be political and administrative. In addition, it was not clear from the documents available to the CJEU that those activities corresponded to the activities mentioned in Article 2(2) (b) and (d) GDPR or could be classified in the same category.
- 4) Finally, the GDPR, in particular in recital 20 and in Article 23, does not provide for any exception with regard to parliamentary activities.

Legal Considerations

Ad 1)

It is true that the definition of the ‘controller’ in Article 4 GDPR does not exclude the area of legislation. However, the scope of a regulation cannot be inferred from a definition alone: The scope of the GDPR is regulated in Articles 2 and 3. The term ‘controller’, as defined in Article 4(7) GDPR, cannot be found in Article 2 GDPR (‘Material scope’) and would therefore only be relevant once the applicability of the GDPR has been clarified.

Ad 2)

The *Lindqvist* judgement cited by the CJEU was based upon the question of whether the publication of personal data by an individual in the context of their voluntary / religious community activity falls under Directive 95/46/EC. At that time, it was argued that if this were accepted, the question of the Directive’s validity would arise, since it was based on Article 100a of the EC Treaty, which concerned measures to harmonize legal and administrative provisions on the establishment and functioning of the common market. Article 3(2) of the Directive provided an exception for an ‘activity which falls outside the scope of Community law’. The CJEU held that the activities cited as

examples in Article 3(2) of the directive were, in any event, ‘activities of the States or of State authorities’ and thus unrelated to individuals’ fields of activity. It must therefore be considered that the exception only applies to activities that are either expressly listed in Article 3(2) or that can be classified in the same category. The CJEU did not consider voluntary or religious community activities to be covered by the exception.

Ultimately, in the *Lindqvist* case, the CJEU (only) examined whether the activity in question was covered by the exception of the Directive. In the present case, too, the essential question concerns the interpretation of the exceptions provided for in Article 2(2) GDPR. To answer it, reference to the (undoubted) suitability of Article 16 TFEU as a legal basis for the GDPR contributes little.

Ad 3)

The CJEU equates the exceptions in Article 2(2) GDPR with those in Article 3(2) of the Directive 95/46/EC, although these are structured differently.

Article 3(2) of Directive 95/46/EC provided:

‘This Directive shall not apply to the processing of personal data:

- *in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,*
- *by a natural person in the course of a purely personal or household activity.’*

In contrast, Article 2(2) GDPR provides:

‘This Regulation does not apply to the processing of personal data:

- a) in the course of an activity which falls outside the scope of Union law;*
- b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;*
- c) by a natural person in the course of a purely personal or household activity;*
- d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’*

Activities that fell outside the scope of Community law were described in more detail in Article 3(2) of Directive 95/46/EC. From this, the CJEU concluded in the *Lindqvist* judgement that the exception applies only to those activities which were expressly listed there or which could be classified in the same category.

According to the GDPR, an activity that falls outside the scope of Union law is, however, a separate exception that is not described more fully in the Regulation (Article 2(2)(a)). Recital 16 gives ‘activities concerning national security’ as an example. Nevertheless, the CJEU stated that an activity covered by the exceptions must belong to those ‘explicitly mentioned by that provision’ (apparently meaning Article 2(2)(b) and (d), see margin no. 71 of the judgement) or be classified in the same category as those. The Court does not seem to attach any individual importance to Article 2(2)(a). However, since activities concerning national security are not listed in Article 2(2)(b) and (d) either, but nevertheless are given as an example of the exception in Article 2(2)(a) in recital 16, it can be assumed that the exceptions may not be interpreted as restrictively as the wording of the judgement suggests.

With reference to the *Lindqvist* judgement, the CJEU also considered whether the activity was characteristic of the State or of a public authority. It stated that while the activities of the Petitions Committee ‘are incontestably public and are activities of that *Land*, that committee contributing indirectly to the parliamentary activity’, the activities are also of a political and administrative nature.

Apparently, the Court assumed that the function of the Petitions Committee is also ‘political as much as administrative’ and therefore not ‘just’ characteristic of the State or public authority. Its conclusion that it is also a characteristic activity of the Federated State is based upon the fact that the committee contributes indirectly (!) to parliamentary activity – however, this was not considered sufficient for the exception to apply.

Ad 4)

Here, the CJEU refers to recital 20 and Article 23 GDPR. Article 23 GDPR determines for which goals and under which conditions the rights of data subjects may be restricted by way of a legislative measure. Restrictions are permitted under certain conditions (necessity, proportionality, etc.) to safeguard national security, the protection of judicial independence and proceedings etc. However, this provision is not declarative of the GDPR’s scope: The applicability of the GDPR to a certain area is a different question than the authorization to provide for restrictions to safeguard a specific sector.

Recital 20 concerns the independence of the judiciary – interestingly, the CJEU does not (also) cite Article 55(3) GDPR, to which recital 20 refers. Article 55(3) GDPR exempts the processing operations of courts acting in their judicial activity from the competence of the supervisory authorities. In principle, however, the GDPR also applies to the activities of the courts and other judicial

authorities – this is even expressly stated in recital 20. There is no such statement concerning the area of legislation.

The fact that parliamentary activities are not explicitly mentioned in recital 20 or in Article 55 GDPR, does not necessarily mean that the GDPR applies to them: If they are not covered by the scope of the Regulation itself, an exception in Article 55 GDPR or recital 20 is not necessary. In any case, from the perspective of the separation of powers, the control of legislative bodies by an administrative authority would be no less problematic than the control of the judiciary.

Conclusions for the Area of Legislation

The significance of this CJEU ruling for the area of legislation/parliamentary activity is difficult to assess. As the above analysis has shown, the crucial argument in this specific case is that the activities of the Petitions Committee are also ‘political as much as administrative’ (and therefore apparently not only ‘characteristic of the State’), hence they do not fall under the exceptions in Article 2(2)(b) and (d) GDPR, nor can be classified in the same category as those.

It should be emphasized that, from the point of view of the CJEU, the activities of the Petitions Committee only ‘indirectly’ contribute to parliamentary activity. The CJEU obviously did not assume that the core area of legislation was affected. Against this background, it seems possible that the CJEU would qualify an activity that is ‘directly’ part of parliamentary activity (i.e. part of the core area of legislation) as a ‘characteristic activity of the State’ and classify it in the same category as Article 2(2)(b) and (d) (or (a)) GDPR. The reasoning on the case at hand leaves this possibility open.

Furthermore, it should be noted that, although the CJEU cited recital 20, it issued no statement on the competence of the supervisory authorities in the area of legislation. The present case arose out of proceedings before an administrative court. The supervisory authority of *Land* Hessen was apparently not involved.

A general conclusion on the applicability of the GDPR in the (core) area of legislation can therefore not be inferred from the present judgement. Only presumptions can be made. Against this background, it seems advisable to monitor further judgements. For Austria, the data protection authority has already decided that its competence is limited to the supervision of particular administrative matters of specific legislative bodies and that there is no further control of the legislature by an executive body.

4. Sarah König (2022)



INTERNATIONAL JOURNAL OF PARLIAMENTARY STUDIES
(2022) 1–11

INTERNATIONAL
JOURNAL OF
PARLIAMENTARY
STUDIES

Case Study



The GDPR's Application and Supervisory Authorities' Remit on National Parliaments' Data Processing in Parliamentary Core Activities

Sarah König | ORCID: 0000-0001-6438-9252
Data Protection Officer Austrian Parliamentary Administration,
Vienna, Austria
sarah.koenig@parlament.gv.at

Abstract

Since the entry into force of the GDPR, national Parliaments within the EU have adopted varying legal opinions on its material scope of application and, *inter alia*, (national) data protection authorities' supervisory jurisdiction concerning data processing in parliamentary core areas. This article summarizes the findings of a European Centre for Parliamentary Research and Documentation (ECPRD) network survey conducted in early 2021 – that is, after the CJEU's decision *Land Hessen* of 9 July 2020, C-272/19. It shows that the judgement had an ambiguous effect on parliaments' legal viewpoints and briefly points out key issues influencing the minority opinion – amongst them the Austrian Parliament's position – that parliamentary core activities' data processing is exempted from the GDPR's scope of application.

Keywords

parliament – GDPR material scope of application – supervisory authorities – survey
– data protection – ECPRD

1 Introduction¹

Parliaments throughout the European Union (EU) generally hold a monopoly over two main competencies: legislation and exercising (political, legal and budgetary) control over the executive. When carrying out these functions, members of parliament, their staff and parliamentary administrations commonly also process personal data, e.g. by publishing deliberations and speeches with direct references to a natural person or items of business such as interpellation (i.e. written questions to the executive in order to monitor executive activities which include personal information). Besides the typical administrative tasks that are similar to any other organisation (e.g. human resources and facility management), parliamentary actors are thus given specific tasks (arguably “powers”) that can be categorized as “parliamentary core activities”.

Whether the General Data Protection Regulation (GDPR)² is also applicable to data processing in those parliamentary core activities has been disputed in parliamentary administrations’ practice and particularly among German-speaking academia. The Court of Justice of the European Union’s (CJEU) decision *Land Hessen* of 9 July 2020, C-272/19, has sparked this debate anew (cf. Meyer 2021, Roßnagel/Rost 2021, Hilbert 2021, Stürmer/Wolff 2021, Heberlein 2021, Grzeszick/Schwartzmann/Mühlenbeck 2020, Pabst 2020). To gain a better and more up-to-date understanding of the approaches of the various Parliaments in this regard, a European Centre for Parliamentary Research and Documentation (ECPRD)³ network survey was started in early 2021. Previous surveys on this topic had been conducted in 2017 and 2018 (the data of the latter are presented in the annexed tabular overview). This article summarizes the findings of the most recent survey (in Part 2.), gives a short analysis of the effect of the *Land Hessen* decision according to the literature, examines the positions of Parliaments before and after it (Part 3.) and lists key issues brought forward by Parliaments which rejected the application of

1 This article is based on findings gathered in course of a European Centre for Parliamentary Research and Documentation’s (ECPRD) network survey and presentation. I thank all responding colleagues and participants for their valuable contribution and ongoing willingness for exchange.

2 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 The ECPRD, established in 1977, connects parliaments whose Presidents are a member of the European Conference of Presidents of Parliament. Its focus on inter-parliamentary cooperation and information exchange is mainly achieved by facilitating comparative studies via information requests and (online) seminars hosted by member Parliaments.

the GDPR to core parliamentary activities (in Part 4.) before outlining conclusions (Part 5.).

2 Survey Outline, Participation and Findings

The representational ECPRD request touched upon two main fields of interest concerning data processing in parliamentary core activities: Firstly, the GDPR's material scope of application (Article 2 GDPR), i.e. whether the GDPR is deemed applicable at all, and secondly, the proceedings of Parliaments concerning the jurisdiction by a supervisory authority mandated by the GDPR (cf. Articles 51 ff and 77 ff GDPR). During the survey and in the ensuing debate thereof, a total of 33 (out of 40 consulted) parliamentary chambers⁴ provided a reply; a tabular overview is given in the Annex to this article.

2.1 GDPR's Application

The GDPR is European Union (EU) secondary law and is based upon Article 7 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union. Article 2 of the GDPR delineates its material scope of application and para (2) foresees exemptions to it, most notably subpara (a), which exempts activities that fall outside the scope of Union law.

According to the ECPRD survey, 22 Parliaments (66.67 % of respondents) consider the GDPR to be applicable to the data processing of parliamentary core activities. However, 7 of the chambers surveyed (21.21 % of total respondents; 31.82 % of GDPR applying respondents) hinted at an indirect application brought about by national stipulations (e.g. Article 2 Belgian Framework Data Protection Law, the Slovene national Personal Data Protection Act and Articles 21–24 Slovene National Assembly Act, the Swedish Chapter 1 Section 2 of Act (2018:218) on Supplementary Provisions to the General Data Protection Regulation). Furthermore, the German Bundestag as well as the Swedish Riksdag explicitly stated that they had not yet settled on a final position on this matter.

Another 7 Parliaments, amongst them both Austrian chambers, deem exemptions of Article 2, especially exemption Article 2 (2) (a) GDPR

⁴ Austria (2), Belgium (2), Bulgaria, Croatia, Cyprus, Czech Republic (2), Denmark, Estonia, Finland, France, Germany (2), Greece, Hungary, Ireland (2), Italy (2), Latvia, Lithuania, Malta, Netherlands (2), Poland – Sejm, Portugal, Romania – Senat, Slovakia, Slovenia – National Assembly, Spain – Congreso de los Diputados, Sweden. The parliament of Luxembourg, Poland's Senat, the Romanian Camera Deputatilor, the Slovene National Council and Spain's Senat did not reply, Norway's Stortinget and the French Senate did not reply substantially.

(potentially) applicable, or in any case deny the Regulation's applicability to core parliamentary activities. In Denmark, the parliamentary work of the Folketinget is *expressis verbis* exempted from GDPR and national data legislation (cf. Section 3 (3) Danish Data Protection Act), while Finland's Data Protection Act expressly exempts parliamentary activities from its application (cf. Section 2 (2) Finnish Data Protection Act). Austria's national Federal Act concerning the Protection of Personal Data (Datenschutzgesetz – DSGVO) stipulates a general extension of the GDPR's material scope of application; nevertheless, the legislator exempted the data processing of parliamentary core activities from this widening of scope by means of a written position during the committee deliberations (cf. Committee Report 2018 p. 5). Whether this approach can prevent the application of the GDPR is currently undergoing judicial review by a pending court case. Certainly, a national constitutional provision (§ 1 DSGVO) granting individuals a constitutional right to privacy and the rights of access, rectification and erasure obliges parliamentary actors in Austria to abide by essential data protection provisions in parliamentary core activities also. The Irish Parliament as well cites abidance by good data protection practice stemming from constitutional principles, nevertheless, such compliance is not considered justiciable. In Ireland, however, Section 60 (1) (a) in conjunction with (3) (a) (i) of the Data Protection Act 2018 stipulates a general restriction of data subjects' rights and obligations in order to safeguard parliamentary privilege (cf. the relevant opening clause Article 23 GDPR).

2.2 *The Jurisdiction of Supervisory Authorities*

The GDPR also mandates the establishment of (at least) one supervisory authority by EU member states to effectively enforce GDPR compliance by, amongst other means and functions, giving it jurisdiction over data subjects' remedies. The specific design of the authority in each state depends on national law; Articles 51 ff GDPR only stipulate the relevant framework.

On the topic of (one or more) supervisory authorities' jurisdiction over the data processing of parliamentary core activities, no Parliament reported that an oversight body had been specially established. The data processing of 20 chambers (60.61 %) is subject to the respective national supervisory authority's remit. In Germany, where more than one such supervisory authority is established, the competence lies with the Federal Commissioner for Data Protection and Freedom of Information. By contrast, 8 Parliaments (24.24 %), amongst them again both Austrian chambers, consider parliamentary core activities' data processing not to be subjected to a supervisory authority's jurisdiction. Most Parliaments (incl. Austria) did not specify the reasons for their position; if they gave any, they centred around strict concepts of the separation of

powers and parliamentary autonomy (see also 4). These issues were especially highlighted by Ireland's Houses of the Oireachtas which are still undecided on the matter. Even the establishment of a discrete (i.e. separate) parliamentary supervisory authority is met with scepticism as the provisions would not sufficiently respect the separation of powers given the imperative provision for a judicial remedy to supervisory authorities' decisions in Article 78 GDPR.

3 Significance of CJEU's Judgement *Land Hessen*

Land Hessen was the first CJEU decision concerning Parliaments' data processing, only the second judgement concerning the GDPR's material scope of application and the first ever that dealt with the activities of a State (authority) where the exemptions laid out in Article 2 (2) (a), (b) and/or (d) are relevant (cf. the shortly after *Land Hessen* published CJEU's judgement of 16 July 2020, *Schrems II*, C-311/18, para. 85). However, the *Land Hessen* decision did not lessen the ambiguity regarding parliamentary core activities, neither concerning the general question of the GDPR's application nor the question of supervisory authorities' jurisdiction:

The Court did, indeed, state that the exemption of Article 2 (2) (a) GDPR must be interpreted restrictively and reiterated arguments from its earlier *Lindqvist* decision concerning Directive 95/46/EC. The data processing by the Petitions Committee of *Land Hessen*'s Parliament was ruled to be undoubtedly characteristic of the State. Nonetheless, the Court found the activity to contribute only "indirectly" to parliamentary procedure and to be as much political as administrative in nature, so the exemption was found to be not applicable (cf. *Land Hessen*, para. 71). In consequence, it remains unclear whether the Court would see the exemption applicable to data processing for activities that "directly" contribute to parliamentary activities. Concerning the topic of supervisory authorities' jurisdiction over parliamentary activities, the *Land Hessen* decision only notes that the GDPR entails no comparable provision to Recital 20. The corresponding Article 55 GDPR excludes judicial activities from a supervisory authority's remit given the principled separation of powers. However, the mere fact that the GDPR entails no such provision concerning the data processing of Parliaments should not lead to the conclusion that the GDPR requests a national supervisory authority's competence over data processing in parliamentary core areas as this would seem no less problematic than such control by the judiciary (cf. Posnik 2021 for an in-depth-analysis of the ruling's legal arguments).

In the German legal literature, the decision met a critical reception: Some are convinced of a general confirmation of the GDPR's material application to data processing in Parliaments given that no exemptions would apply (cf. Heberlein 2021). Others support the decision's tenor of the GDPR's application, although its line of argumentation, especially the Court's cumulative requirements for Article 2 (2) (a) to be applicable that effectively demand a fulfilment of exemptions Article 2 (2) (a) and (b) or (d), was criticised (cf. Meyer 2021, Stürmer/Wolff 2021). Others simply reject the Court's reasoning based on the main argument that the Court would overstretch its competences (cf. Grzeszick/Schwartzmann/Mühlenbeck 2020, Roßnagel/Rost 2021), even raising the possibility of a (controversial) "ultra-vires"-control (cf. Pabst 2020).

The ambiguous impression concerning *Land Hessen's* influence on the GDPR's application in the Parliaments is also supported by a comparative examination of their positions in 2018 and 2021: Of 21 Parliaments that provided replies in both ECPRD surveys, 7 chambers (33.33 %) changed their stance concerning the GDPR's application on data processing in parliamentary core activities. Of these, only 3 Parliaments shifted their position from a previous approach of non-application to that of application (14.29 %), one of which (Estonia) also referenced the decision *Land Hessen* in their 2021-reply. 2 chambers (9.52 %) simply revoked the previously stated provisional nature of the GDPR's application and another 2 chambers (9.52 %) now regard parliamentary core activities' data processing as being exempted from the application of the GDPR. Also, when examining the 12 Parliaments that did not provide a reply in 2018 only half of them now apply GDPR to data processing in parliamentary core areas with the German Bundestag being the only chamber directly referencing an ongoing assessment of *Land Hessen's* impacts.

In the meantime, the CJEU has issued another judgement dealing with the GDPR's material scope of application and the exemption of Article 2 (2) (a), although not in direct reference to parliamentary activity. Still, in its decision of 22 June 2021, C-439/19, *Latvijas Republikas Saeima (Points de pénalité)*, the Court sets forth further parameters for activities that can be considered to aim at safeguarding national security and are thus relevant for the exemption of Article 2 (2) (a) GDPR, namely, "those that are intended to protect essential State functions and the fundamental interests of society" (cf. para. 67).

4 Key Issues with the GDPR's Application to Parliamentary Core Activities

As previously mentioned, hardly any of the Parliaments, including the Austrian, explained their positions on the topic areas inquired about. However,

amongst the Parliaments that deny the GDPR's application to parliamentary core activities' data processing, the prerogative of Parliaments to organise and decide on procedural and internal affairs without any executive or judicial oversight seems to be the most common underlying argument. This "parliamentary autonomy" or "parliamentary privilege" (in Austria mostly discussed in the context of members of Parliament's "immunity") is deduced from a (strict) concept of separation of powers that aims at upholding Parliaments' functioning on an institutional level. This aspect can amount to a national constitutional principle that must be considered accordingly when assessing conflicting interests. The Court's latest interpretation of Article 2 (2) (a) GDPR, i.e. excluding activities intended to protect an essential State function from the GDPR's application (see above 3.), strengthens the view that a Parliament's data processing in core activities can be considered outside the scope of Union law. Such an interpretation would also not come into conflict with the principled primacy of the application of EU law.

The GDPR – when considered applicable – allows for the establishment of distinct and special oversight bodies as well as normative adaptations (including for parliamentary activities) which a variety of Parliaments applying the GDPR have made use of (e.g. definitions of "controllers", the stipulation of lawful data processing, restrictions of data subjects' rights). Notwithstanding these options the scope of Union law does not comprise national parliamentary procedure and any conditions thereto encroach on the autonomy of national Parliaments, especially mandatory remedies as foreseen by Articles 77 ff GDPR.

In this context, a pending decision by the Austrian Supreme Administrative Court seems noteworthy: A decision of the Austrian Federal Administrative Court granting the Austrian Data Protection Authority (ADPA) competence to decide on data processing by an investigative committee of the National Council, more specifically the publication of an informant's data in the committee's minutes (undoubtedly a parliamentary core activity) was challenged by the ADPA itself. According to the ADPA's argumentation, control by executive bodies in form of supervisory authorities like itself over parliamentary core activities should be excluded from the outset given the inherent European model of separation of powers. Therefore, exemptions as foreseen by the GDPR for the judicial activity of courts would also be superfluous when activities of the legislature are concerned.

The Austrian Supreme Administrative Court has recently initiated a reference for a preliminary ruling by the CJEU in this matter (cf. C-33/22, *Österreichische Datenschutzbehörde*). The reference also includes questions concerning the application of the GDPR, specifically whether national Parliament's data processing in core activities can be considered to fall outside the scope of Union law and therefore be exempted from the GDPR.

5 Conclusion and Outlook

The National Parliaments' legal viewpoints concerning the GDPR's application on data processing in parliamentary core activities, i.e. activities that directly contribute to legislation, and supervisory authorities' jurisdiction thereto remain diverse 3 years after the GDPR has taken effect. However, a clear majority of Parliaments currently does apply GDPR norms (indirectly) and considers their data processing to be subjected to executive and judicial oversight. The CJEU's *Land Hessen* decision ultimately did not have a harmonizing effect in this context; whether potential future jurisprudence can remove current uncertainties remains to be seen especially in light of the recently introduced reference for a preliminary ruling "Österreichische Datenschutzbehörde" (C-33/22).

With regard to the minority position also shared by the Austrian Parliament which considers data processing in parliamentary core activities as being excluded from the GDPR's material scope of application, the available CJEU's decisions demand a differentiated assessment of data processing activities given the distinctive criteria of indirect and direct contributions to parliamentary procedure as well as those activities that are aimed at protecting essential State functions and the fundamental interests of society. Once again, data protection legislation proves to be extremely nuanced. Parliaments' continued exchange of views and practice on this matter is therefore of the utmost importance not only to parliamentary actors but also to data subjects whose right to privacy is fundamentally protected by European law.

Annex

TABLE 1 Parliamentary chambers applying the GDPR in parliamentary core areas and acknowledging supervisory oversight in this context.

Parliamentary chamber	GDPR application		Supervisory authority's remit
	2018	2021	
Austria (National Council, Federal Council)			
Belgium (Chambre des Représentants, Sénat)	X	X	X
Bulgaria (National Assembly)	no reply	X	X
Croatia (Hrvatski Sabor)	no reply	undefined	X
Cyprus (House of Representatives)	no reply	undefined	
Czech Republic (Chamber of Deputies, Senat)	X	X	X
Denmark (Folketinget)	no reply		
Estonia (Riigikogu)		X	undecided
Finland (Eduskunta)			
France (Assemblée Nationale)	X	X	X
Germany (Bundesrat)	(X)	X	X
Germany (Bundestag)	no reply	(X)	X
Greece (Voulí tōn Ellínōn)	undecided	X	X
Hungary (National Assembly)	X	X	X
Ireland (Houses of the Oireachtas)	undecided		undecided
Italy (Camera Dei Deputati)	no reply	X	
Italy (Senato della Repubblica)	no reply	undefined	
Latvia (Saeima)	X	X	X
Lithuania (Seimas)	no reply	X	X
Malta (House of Representatives)	no reply		
Netherlands (Eerste Kamer der Staten-Generaal, Tweede Kamer der Staten-Generaal)	no reply	X	X
Poland (Sejm)	X	X	X
Portugal (Assembleia da Republica)	X	X	X
Romania (Senat)	no reply	undefined	undefined
Slovakia (National Council)	(X)	X	X

TABLE 1 Parliamentary chambers applying the GDPR in parliamentary core areas and acknowledging supervisory oversight in this context. (*cont.*)

Parliamentary chamber	GDPR application		Supervisory authority's remit
	2018	2021	
Slovenia (National Assembly)	X	X	X
Spain (Congreso de los Diputados)		X	undefined
Sweden (Riksdag)	(X)	(X)	X

SOURCE: REPLIES PROVIDED BY PARLIAMENTS TO ECPRD REQUESTS 3890 (2018) AND 4673 (2021).

References

Legislative Material

Committee Report (2018): Austrian Constitution Committee's Report 98 annex to the Stenographic Records xxvi. Legislative Period, *available online*: <https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00098/fname_689501.pdf> (in German, last accessed 12 January 2022).

Judicature

CJEU, 9 July 2020, C-272/19, *Land Hessen*, *available online*: <<https://curia.europa.eu/juris/document/document.jsf?text=&docid=228367&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=483451>> (last accessed 12 January 2022).

CJEU, 16 July 2020, C-311/18, *Schrems II*, *available online*: <<https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=193058>> (last accessed 12 January 2022).

CJEU, 22 June 2021, C-439/19, *Latvijas Republikas Saeima (Points de pénalité)*, *available online*: <<https://curia.europa.eu/juris/document/document.jsf?text=&docid=243244&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=193058>> (last accessed 12 January 2022).

Literature

Grzeszick, Bernd, Schwartmann, Rolf, and Mühlenbeck, Robin L. (2020). Nationale Parlamente und DS-GVO: Die unzutreffende Sicht des EuGH. *Neue Zeitschrift für Verwaltungsrecht* 20/2020, pp. 1491–1495.

Heberlein, Horst (2021). Bereichsausnahme für Parlamente? Geltung der DS-GVO für parlamentarische Tätigkeiten. *Zeitschrift für Datenschutz* 2/2021, pp. 85–88.

- Hilbert, Patrick (2021). Der Datenschutz der Parlamente. *Neue Zeitschrift für Verwaltungsrecht* 16/2021, pp. 1173–1177.
- Meyer, Stephan (2021). Die Anwendung der Datenschutz-Grundverordnung auf Parlamente – Der EuGH und die Auslegungsfigur *Eiusdem Generis*. *Deutsches Verwaltungsblatt* 22/2021, pp. 1476–1482.
- Pabst, Heinz-Joachim (2020). Die (Nicht-)Geltung der DS-GVO für die Arbeit der Parlamente und ihrer Ausschüsse. *Recht der Datenverarbeitung* 5/2020, pp. 249–254.
- Posnik, Rosi (2021). Legal Considerations on the CJEU Judgement of 9 July 2020, C-272/19. *International Journal of Parliamentary Studies* 1/2021, pp. 154–159.
- Roßnagel, Alexander, and Rost, Maria Christina (2021). Ist die Datenschutz-Grundverordnung auch in den Landtagen anwendbar? Demokratische Souveränität und Unionsdatenschutz. *Neue Zeitschrift für Verwaltungsrecht* 22/2021, pp. 1641–1646.
- Stürmer, Verena, and Wolff, Heinrich Amadeus (2021). Die parlamentarische Datenverarbeitung und die Datenschutzgrundverordnung. Zugleich Anmerkungen zu EuGH, Urt. v. 9.7.2020, C-272/19, VQ gegen Land Hessen. *Die Öffentliche Verwaltung* 4/2021, pp. 167–171.