28.08.2024

Landvurdering

Google Workspace for Education i Taiwan

Innhold

1. Innledning

1.1. Beskrivelse av overføringen og formålet med landvurderingen

Norske kommuner benytter skytjenester under Google Workspace for Education ("**GWE**") i grunnskolen. Dette innebærer at det blir behandlet personopplysninger om elever, foresatte og ansatte. Ved bruk av Google-tjenesten vil det skje overføringer til eller fjerntilgang fra som ikke er omfattet av en adekvansbeslutning fra EU-kommisjonen i henhold til GDPR artikkel 45.

Bruk av GWE innebærer at Google lagrer data på servere i Taiwan. Overføringene gjelder personopplysninger om norske brukere av Google Workspace for Education, herunder elever, lærere og foresatte. Overføringene vil skje på fortløpende basis. Personopplysningene behandles lokalt og på dataservere i Norge/EU, men kan bli overført til Taiwan for formål knyttet lagring (skylagring hvor dataene ligger fysisk på en server i Taiwan.

Kommunen er behandlingsansvarlig for disse overføringene og må derfor vurdere risikoen ved overføringene, samt inngå nødvendig Standard Contractual Clauses ("**SCC**") som publisert av EU-kommisjonen og gjennomføre en Transfer Impact Assessment ("**TIA**") med implementering av nødvendige sikkerhetstiltak for overføringene dersom SCC ikke i seg selv er tilstrekkelig.

Denne landvurderingen skal gi kommunene veiledning i hvordan å vurdere beskyttelsesnivå og sikkerhetstiltak for Taiwan slik at kommunen selv kan gjennomføre en TIA. For å vurdere beskyttelsesnivået ved overføringene må kommunen vurdere lovgivningen og rettspraksis i importlandet, og denne landvurderingen gjennomgår relevant lovgivning i Taiwan som påvirker personvernet for norske registrerte.

1.2. Rettslig rammeverk

De primære rettsaktene som regulerer myndighetenes inngripen i personopplysninger på Taiwan, er:

- **Personal Data Protection Act (PDPA)**, se punkt 3.1.
- **Communication Security and Surveillance Act (CSSA)**, se punkt 3.2.
- **Telecommunications Act (TA) og Telecommunications Management Act (TMA)**, se punkt 3.3.
- **Grunnlov eller andre tilknyttede traktater og konvensjoner**

I tillegg kommer **Code of Criminal Procedure (CCP)** og **Police Power Execise Act (PPEA)**, men disse er ikke vurdert i detalj nedenfor.

1.3. Øvrige kilder

Dataguidance/Datagovernance – DataGuidance er en sentralisert, regulatorisk forskningsplattform bygget av et nettverk av interne forskere, juridiske eksperter og oversettere.[1]

«Taiwan Internet Transparency Report» - Forskningsrapport publisert av Taiwan Association for Human Rights.[2]

Annet – Øvrig faglitteratur, fagartikler og andre relevante kilder (se noter)

[1] https://www.dataguidance.com/
[2] https://transparency.tahr.org.tw/TITR_Report_2015_en.pdf

1.4. Avgrensninger og forbehold

Denne landvurderingen dekker kun regelverk og praksis som var offentlig eller kjent for prosjektet og relevant for vurderingene.

Vi gjør også oppmerksom på at rettskilder og praksis kan være utdatert, endret eller faset siden landvurderingen tilgjengeliggjøres.

Konklusjonene i denne landvurderingen baserer seg på prosjektets tolkning og vurderinger av Taiwansk rett og praksis.

2. Oppsummering og konklusjon

Landvurderingen gir en vurdering av Taiwans lovgivning og praksis knyttet til personvern og overvåkning, spesielt i lys av norske skolers bruk av Google Workspace for Education (GWE). Hovedfunnene indikerer at selv om Taiwan har gjort flere endringer i sin lovgivning for å styrke personvernet, er det fortsatt utfordringer knyttet til overvåkning og beskyttelse av personopplysninger.

Det er identifisert at Communications and Surveillance Act (CSSA) ikke fullt ut oppfyller de grunnleggende europeiske garantiene, spesielt når det gjelder uavhengig tilsyn og effektive rettsmidler. Dette kan påvirke beskyttelsesnivået for personopplysninger overført til Taiwan.

Prosjektet anbefaler at kommuner som bruker GWE må vurdere risikoen ved overføringer til Taiwan og implementere nødvendige sikkerhetstiltak. Dette kan inkludere inngåelse av Standard Contractual Clauses (SCC) og gjennomføring av en Transfer Impact Assessment (TIA).

Videre bør det tas hensyn til praksis og håndheving av lovgivningen, som rapporten fra Taiwan Association for Human Rights (TAHR) og Googles Transparency Reports indikerer kan være mangelfull.

Til slutt konkluderer landvurderingen med at er det behov for ytterligere tiltak for å sikre et tilstrekkelig beskyttelsesnivå for personopplysninger overført til Taiwan.

3. Beskrivelse av relevante regelverk i Taiwan

3.1. Personal Data Protection Act (PDPA)

3.1.1. Lovens materielle virkeområde

Personal Data Protection Act gjelder beskyttelse av personopplysninger i Taiwan. All innsamling, behandling og bruk av personopplysninger i Taiwan er underlagt reglene i PDPA og «Enforcement Rules».[3] Regelverket ble satt i kraft i 2015. Taiwan er ikke omfattet av en adekvansbeslutning fra EU-kommisjonen.

I henhold til artikkel 51 paragraf 2 i PDPA, sammenholdt med utredningen fra kompetent autoritet (FA-Lu-Zi No. 10403509750 datert 26.august 2015), omfatter PDPA all innsamling («collection»), behandling («processing»), og eller bruk («use») av personopplysninger innenfor Taiwansk territorium – uavhengig av om de registrerte («data subjects») er lokalisert i Taiwan eller ikke. [4]

Med behandling («processing») av personopplysninger menes «recording», «inputting», **«storing»**, «compiling/editing», «correcting», «duplicating», «retrieving», «deleting», «outputting», «connecting». Med bruk («use») menes håndtering av personopplysninger via alle andre metoder utenom det som nevnes under begrepet «processing».

Overføring av personopplysninger om norske brukere av GWE til datasenter i Taiwan vil med dette utgjøre en behandling («processing») av personopplysninger som dekkes av PDPA.

3.1.2. Myndighetenes tilgang til overførte data

Kapittel 2 i PDPA regulerer innsamling og håndtering av data som faller utenfor bestemmelsene i kapittel 1. Dette omfatter bl.a. innsamling av data som er nødvendig av hensyn til nasjonal sikkerhet eller i et straffeforfølgelsesøyemed.

Artiklene 15 og 16 utgjør rammene for slik behandling. Etter artikkel 15 er behandling av personopplysninger utenom kap.1 kun lov dersom ett av tre vilkår er oppfylt: Nødvendig for en lovbestemt forpliktelse for staten, samtykke, eller at datasubjektets rettigheter og interesser ikke blir krenket. Artikkel 16 fastsetter hvilke lovlige formål en slik behandling kan ha. De mest relevante formålene er at behandlingen er lovpålagt, og at behandlingen er nødvendighet for nasjonal sikkerhet eller offentlige interesser. Begge artiklene 15 og 16 referer til øvrige nasjonale regler generelt. Vi viser til punkt 1.2 over for en oversikt, og ellers til vurderingen av disse nedenfor.

Private virksomheter og organisasjoner kan ikke motsette seg begjæringer om innsyn eller inndrivelse av data fra statlige myndigheter. Organisasjoner kan imidlertid sende klage til kompetent autoritet, dersom de mener begjæringen er ulovlig. Dersom en klage ikke fører frem, kan organisasjonen klage saken videre for relevant nasjonal domstol/domstolslignende organ. Ordlyden er ellers taus når det gjelder de nærmere ramme og rekkevidde av Taiwans myndighet til å inndrive data.

3.1.3. Lovlig behandlingsgrunnlag

I henhold til PDPA kapittel 1 har staten tilgang på personopplysninger og behandling begrenset til tilfeller der følgende vilkår er oppfylt:

1) Der dette er nødvendig for utøvelse av lovpålagte forpliktelser hos staten.
2) Der samtykke er gitt fra individet (datasubjektet), og;
3) Der rettighetene og interessene til datasubjektet ikke er krenket

[3] https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021, artikkel 1
[4] Ibid, artikkel 51 paragraf 2

3.1.4. Prinsipper, rettigheter og øvrige begrensninger for behandling av personopplysninger

PDPA inneholder overordnede prinsipper for etterlevelse av regelverket. Prinsippene listes opp i ulike bestemmelser.[5] Prinsippene inkluderer krav til forholdsmessig, adekvat og relevant behandling av data; formålsbegrensing, nødvendighet og forholdsmessighet for behandlingene; særlige regler for sensitive personopplysninger og øvrige prinsipper som finnes igjen i GDPR.[6]

3.1.5. Håndheving, kontroll og prøving av rettigheter

Det eksisterer ikke en dedikert, uavhengig og kontrollerende aktør tilsvarende europeiske datatilsyn. Senere endringer ved PDPA har imidlertid formalisert etableringen av et slikt organ. Dette organet skal kalles Personal Data Protection Comission (PDPC), men er enda ikke virksomt i praksis.[7]

National Development Council (NDC) skal håndheve og avsi beslutninger på saker på PDPAs område, samt kompetanse til å tolke både PDPA og de interne prosedyrene som statlige aktører er forpliktet til å etablere under PDPA.

3.1.6. Tilnærming til GDPR og adekvansbeslutning

PDPA har vært gjenstand for flere endringer siden ikraftsettelse i 2015. Deler av disse endringene kan trolig spores tilbake til europeisk innflytelse og inspirasjon fra GDPR som lovverk.[8] Det er grunn til å tro at Taiwanske myndigheter har en ambisjon om å oppnå adekvansbeslutning fra EU.[9] Siden 2015 er det holdt flere offentlige høringer. Målet med høringene er å utbedre PDPA på en demokratisk måte. [10] Det er ikke kjent for prosjektet om, eller eventuelt hvor i prosessen EU er med å godkjenne Taiwan som lovlig importør av overførte personopplysninger.

3.2. Communication Security and Surveillance Act

3.2.1. Lovens materielle virkeområde

Communication Security and Surveillance Act ("**CSSA**") autoriserer statlig overvåkning av kommunikasjon som vurderes relevant inn mot politi- eller annen statlig iverksatt etterforskning.

Formålet med regelverket er som følger:

> «This Act is enacted to safeguard the freedom of private communications and privacy, to protect from unlawful intrusion, and to ensure national security and maintain social order.» (jf. Artikkel 1)

I henhold til artikkel 13 bør («should») overvåkning gjennomføres ved «intercepting, wiretapping, sound recording, video recording, photographing, opening, checking, copying communications or other similar necessary methods […]». CSSA gir ingen klar anvisninger på skillet mellom målrettet overvåkning og såkalt bulk-innsamling av data og hjemlene for dette.

3.2.2. Statlig tilgang til overførte data

Overvåkning etter CSSA er ikke begrenset til informasjon om- eller kommunikasjon fra/mellom innbyggere i Taiwan. Etter artikkel 7 kan målet for en bestemt overvåkningsaktivitet være;

- «Domestic communications of foreign forces, hostile foreign forces, or their agents»,
- «Cross-border communications of foreign forces, hostile foreign forces, or their agents»,

---

[5] https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021, se nevnte artikler
[6] For prinsipper og rettigheter se artiklene 3, 5, 6, 8, 9, 10, 11, 18 og 19.
[7] Taiwan - Data Protection Overview | Guidance Note | DataGuidance, punkt 1.1, 3.1
[8] Taiwan - Data Protection Overview | Guidance Note | DataGuidance, se punkt 1.1
[9] Se note 5
[10] Se note 5

- «Off-shore communications of foreign forces, hostile foreign forces, or their agents»

Begrepet «foreign forces» defineres i artikkel 8. Med «foreign forces» menes:

- «Foreign governments, foreign or overseas political entities, their subordinate organizations or representative agencies»
- «Organizations under the direction or control of foreign governments, foreign or overseas political entities»
- «Organizations with the aim of operating international or cross-border terrorist activities»

Begrepet «agent of foreign forces or offshore hostile forces» defineres i artikkel 9 som:

- «A person who participates, coerces others, or abets others in gathering secret intelligence, or other secret intelligence activities for foreign forces or offshore hostile forces, that risk endangering national security.»
- «A person who participates, coerces others, or abets others in sabotage or cross-border terrorist activities for foreign forces or offshore hostile forces.
- «A person who serves as an official, or an employee for foreign forces or offshore hostile forces, or as a member of an international terrorist organization.»

3.2.3. Lovlig behandlingsgrunnlag

Overvåkning etter CSSA krever at flere rettslig vilkår er oppfylt. Etter artikkel 5 (1) i CSSA følger det overvåkningen være rettet mot «communications», eller «communications records». Med «communications» menes «[u]tilizing wired and wireless telecommunication equipment to send, store, transmit, or receive symbols, texts, images, sound or other types of information» jf. artikkel 3 nr. 1. Her inkluderes også post og brev («Mail and letters»), samt tale og samtaler («Speeches and conversations») jf. nr. 2 og nr. 3. Med «communications records» menes datatyper som masterdata og metadata. I artikkel 3-1 beskrives dette som «[…] records such as the telecommunications numbers of the sender and the recipient, time of communication, length of use, address, service type, mailbox or location information generated by the telecommunications system after the telecommunications user uses the telecommunications services.».

Etter ordlyden i artikkel 5 omfatter CSSA det meste av data som naturlig faller inn under begrepet kommunikasjon, herunder både digital og analog kommunikasjon. Hjemmel og autorisasjon til overvåkning gis kun i saker som er av en strafferettslig karakter eller som er straffebelagt etter taiwansk lov.[11]

3.2.4. Prinsipper, rettigheter og øvrige begrensinger

Overvåkningen må være nødvendig og forholdsmessig. Etter artikkel 2 følger det at: «The surveillance mentioned in the preceding Paragraph shall not exceed the necessary limits to achieve the objective, and the appropriate methods for the action should have only the minimum intrusion.».

3.2.5. Håndheving, kontroll og prøving av rettigheter

Etter artikkel 5 (2) følger det videre at ingen overvåking kan igangsettes uten godkjenning, eller uten en «interception warrant», fra «the court». Det er ikke klart hvilken domstol eller aktør med domstolsmyndighet som begrepet «the court» henviser til. Det kan likevel antas at dette gjelder samtlige alminnelige domstoler i Taiwan som har kompetanse til å avsi dommer på strafferettens område. Mer om domstolskontroll under punkt 4.

[11] Se note 6, se særlig artikkel 5 og artikkel 6.

3.3. Telecommunications Act og Telecommunications Management Act

3.3.1. Lovenes materielle virkeområde

Telecommunications Act ("**TA**") trådte i kraft i 1996, men er senere erstattet med Telecommunications Management Act ("**TMA**") i juli 2020.[12] Regelverkets formål var å sikre trygg utvikling av telekommunikasjon, fremme offentlig velferd, sikre beskyttelsen av kommunikasjon, samt å verne rettighetene og interessene til brukere av telekommunikasjonstjenester i Taiwan. [13]

TMA viderefører og utvider TAs formålsbestemmelse. Dette gjelder også store deler av TAs øvrige bestemmelser. Til tross for stor grad av videreføring, må inntoget av TMA regnes som en betydelig lovendring i Taiwan. Av interesse for prosjektet er det særlig endringer i hjemlene for utleveringsbegjæringer fra statlige aktører i TA.

3.3.2. Statlig tilgang til overførte data etter TA

Det følger av artikkel 7 i TA at en «[…]telecommunications enterprise or its employees, including the retired, shall hold the existence and contents of communications in strict confidence.»

Etter ordlyden gjelder her en hovedregel om plikt til arkivering og sikring av data innhentet og lagret i forbindelse med bruk av elektroniske verktøy i Taiwan. Unntak til denne hovedregelen utløses dersom «the disclosure of such records» gjennomføres i tråd med anvendelige lover og reguleringer. Hvilke anvendelige lover og reguleringer dette gjelder, nevnes ikke spesifikt. En antakelse er likevel at dette er en implisitt henvisning til CCP og CSSA, slik som i PDPA.

Artikkel 3 i «Regulation for Handling Requests from Competent Aurhorities for Comm. Rec.» skal også være relevant i denne sammenheng. Ifølge J.Marshall involverer inngangsvilkårene for utlevering en «[…]«easy -to-meet» standard that only requires the applicant agency to state the necessity, reasonableness, and proportionality when requesting the records.».[14] Prosjektet er ikke i stand til å verifisere om denne forståelsen stemmer. Dette skyldes at nevnte regulering ikke lenger er tilgjengelig – trolig fordi TA ble erstattet med TMA i 2020.

3.3.3. Statlig tilgang til overførte data etter TMA

Hovedregelen om arkivering og sikring av «records» er videreført i TMA – riktignok i en litt annen språkdrakt, se beskrivelse artikkel 7 i TA over. TMA ser ikke ut til å videreføre unntaket om utleveringer til statlige aktører. Unntak til hovedregelen kan fremdeles inntre, men her er vilkårene endret. Når det gjelder utlevering av data til statlige aktører, henvises det til relevante bestemmelser og unntak i CSSA, se artikkel 9 siste ledd. Her følger at «[t]elecommunications enterprises and those who have established PSTN are obliged to assist in the implementation of communication surveillance and in the access of communications records and communications user's information in accordance with the Communication Security and Surveillance Act.".

---

[12] https://www.leeandli.com/EN/NewslettersDetail/6496.htm og https://freedomhouse.org/country/taiwan/freedom-net/2021 om at TMA erstatter TA.

[13] https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060001, Article 1.

[14] Se «Eyes on the Road Program in Taiwan—Information Privacy issues under the Taiwan Personal Data Protection Act, 31 J. Marshall J. Info. Tech. & Privacy L. 145» (2015), John Marshall Journal of Information Technology and Privacy Law er en lovgjennomgang publisert av en studentgruppe ved John Marshall Law School. Publikasjonene dekker internasjonal informasjonsteknologi og personvernlovgivning. https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1758&context=jitpl, side 171.

4. Landvurderingen - Taiwan

4.1. Overordnet problemstilling og metode

I henhold til steg 3 i EDPBs «Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0» er formålet med en landvurdering å avgjøre om det finnes lovgivningen og/eller praksis i landet det overføres personopplysninger til som påvirker effektiviteten til overføringsgrunnlaget som er valgt.[15] Analysen skal fokusere på lokale lover og regler som er relevante for overføringen og overføringsgrunnlaget. Med hensyn til den konkrete overføringen skal følgende spørsmål svares ut:

- Kan dataimportøren garantere et tilstrekkelig beskyttelsesnivå for personopplysningene som overføres til tredjelandet (Taiwan)?

Hvorvidt et tredjeland kan vurderes til å ha tilstrekkelig beskyttelsesnivå avhenger av:

1) Om lokal overvåkningslovgivning gjelder for den konkrete overføringen – og hvis ja;

2) Om de såkalte "grunnleggende Europeisk garantiene" er oppfylt for myndighetenes tilgang til personopplysninger med grunnlag i den/de aktuelle loven(e). [16]

De grunnleggende Europeiske garantiene baserer seg på EU-charteret slik det er tolket av EU-domstolen. Her reflekteres blant annet den grunnleggende retten til privatliv. Denne retten kan også finnes i artikkel 8 i Den Europeiske Menneskerettighetskonvensjonen ("**EMK**") som er inkorporert i Grunnloven.

Ifølge EDPB kan de fire kategorier grunnleggende garantier beskrives slik:

- **Garanti A**: Behandlingen (tilgangen) må være basert på klare og presise regler som er tilgjengelige for offentligheten.
- **Garanti B**: Behandlingen (tilgangen) må være nødvendig og proporsjonal for å oppnå et legitimt formål.
- **Garanti C**: Det må være et uavhengig tilsynsorgan som kan gjennomgå bruken av tilgangen.
- **Garanti D**: De registrerte personene må ha tilgang til effektive rettsmidler dersom deres rettigheter har blitt krenket som følge av myndighetenes tilgang.

Hvis alle fire kategorier garantier er til stede, er personopplysningene godt nok beskyttet ved en overføring. Dersom minst én av garantiene ikke er til stede, må det gjennomføres ytterligere tiltak for å gi personopplysningene et tilstrekkelig beskyttelsesnivå.[17]

Landvurderingen inkluderer videre en gjennomgang av hvordan regelverkene gjennomføres og håndheves i praksis. Praksis vil i denne landvurderingen benyttes til to ulike formål avhengig av om de grunnleggende garantiene vurderes oppfylt eller ikke. Dersom regelverkene man vurderer ikke oppfyller de grunnleggende garantiene, skal beskrivelse av praksis brukes som et faktagrunnlag inn mot identifiseringen av aktuelle kompenserende sikkerhetstiltak. Dersom regelverkene man vurderer

[15] https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[16] European Essential Guarantees. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
[17] Ibid.

oppfyller de grunnleggende garantiene, skal beskrivelse av praksis brukes for å verifisere at regelverkene faktisk håndheves slik loven sier.

4.2. Regelverk som gjelder for overføringen til Taiwan

4.2.1. Communications and Surveillance Act (CSSA)

Det er ikke tvilsomt at personopplysninger lagret om norske brukere på datasenter i Taiwan omfattes av kommunikasjonsbegrepet slik det er definert i CSSA artikkel 3, 3-1. Det Det er også klart at norske brukere av GWE omfattes av begrepet "Foreign Forces" i artikkel 8.

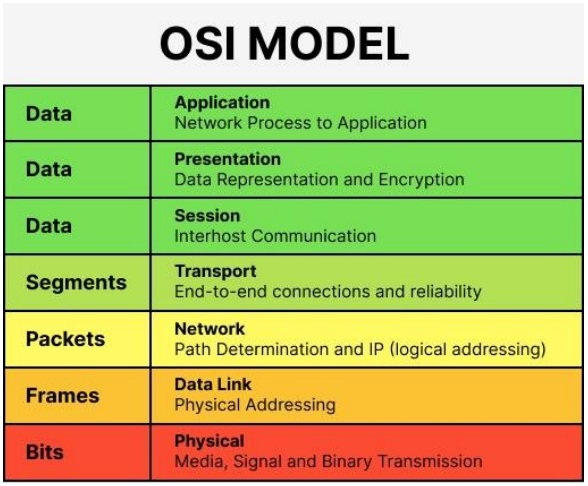
Prosjektet legger med dette til grunn at CSSA kan komme til anvendelse på data om norske brukere av GWE lagret i Taiwan.

4.2.2. Telecommunications Act (TA) og Telecommunications Management Act (TMA)

TMA og TA inneholder bestemmelser som har til formål å sikre statens mulighet til å inndrive kommunikasjon og annen data inn mot ulike statlige etterforsknings- og/eller overvåkningprosesser. I praksis involverer dette tvungen assistanse og tilgjengeliggjøring av systemer og infrastruktur slik at kommunikasjon og data kan deles. I det videre vil TMA og TA vurderes likt.

I den forbindelse er det «telecommunication enterprises», eller telekommunikasjonsoperatører som er pliktsubjekter etter TMA og TA. Begrepet telekommunikasjonsoperatør omfatter aktører som er registrert i tråd med «Act to provide telecommunications services», og som leverer «telecommunications services».

Telekommunikasjonstjenester («telecommunications services») begrenses videre til telekommunikasjon overført via «PSTN» (Public Switched Telephone Network) - oversatt til det linjesvitsjede telefonnettverket (mobil- og fasttelefonnettverket). PSTN utgjør den fysiske telekominfrastrukturen. Slik prosjektet ser det er PSTN en fastlinjebasert, tradisjonell telefonitjeneste, ikke en skylagringstjeneste. Prosjektet mener derfor at den bestemte tjenestekonfigurasjonen av Google Workspace for Education i norske skoler ikke kvalifiserer som PSTN i Taiwan.



(https://cdn.codegym.cc/images/article/3effcdd0-5b89-4574-b154-c2c1c65d945d/512.jpeg)

Bruk av Google Workspace for Education med skylagring i Taiwan vil med andre ord falle utenfor regelverkets virkeområde. Lokal ekspertise i Taiwan ved Advokatfirmaet Nishimura & Asahi Taiwan støtter denne forståelsen, se vedlegg.

Prosjektet legger med dette til grunn at TMA og TA ikke vil komme til anvendelse på personopplysninger om norske brukere av GWE lagret i Taiwan.

4.3. Vurdering av regelverkene som gjelder for overføringen

4.3.1. Communications and Surveillance Act (CSSA)

4.3.1.1. Garanti A: Klare og presise regler som er tilgjengelige for allmennheten.

Det europeiske personvernrådet oppsummerer i sin veiledning noen sentrale momenter når tilstedeværelsen av de fire garantiene skal vurderes. Veiledningen er bl.a. basert på rettspraksis fra Court of Justice European Union (CJEU) og European Court of Human Rights (ECtHR). [18]

I vurderingen av garanti A er følgende spørsmål og vurderingstema av betydning:

1) Er hjemlene for overvåkning tilstrekkelig klare og presise når det gjelder inngrepenes rekkevidde og omfang? [19]
2) Er det tilstrekkelig klarlagt når overvåkning kan finnes sted, herunder hvilke situasjoner og omstendigheter som kan være rettslig utløsende for overvåkning? [20]
3) Er begrensninger i de registrertes mulighet til å gjøre sine rettigheter gjeldende inkludert og synliggjort i den aktuelle lovgivningen? [21]
4) Kravene til presisjon og tilgjengelighet etter punkt 1 skal vurderes og overholdes likt på tvers av ulike statlige overvåkningsprogram. Hjemler for bulk-innsamling av data er følgelig underlagt de samme krav til klarhet og presisjon som hjemler for målrettet overvåkning.[22]
5) Er individet/individene som overvåkes i stand til å forutse konsekvensene av et inngrep i henhold til aktuell overvåkningslovgivning? Kravet til forutsigbare regler må rimeligvis avgrenses mot behovet for hemmelighold og hensynet til nasjonal sikkerhet. [23]

Communications and Surveillance Act har til formål å sikre fri privat kommunikasjon, hindre ulovlig inntrengsel, og å ivareta nasjonal sikkerhet og sosial orden (prosjektets oversettelse) jf. artikkel 1. Regelverket autoriserer statlig overvåkning av kommunikasjon som vurderes relevant inn mot politi- eller annen statlig iverksatt etterforskning.

Når det gjelder inngrepenes rekkevidde og omfang, definerer artikkel 3 og artikkel 13 overvåkningsmetode og rekkevidde (se gjennomgang i punkt 3.2.3). Artikkel 3-1 beskriver omfanget av overvåkningen. Artikkel 5 i CSSA beskriver nærmere de omstendigheter som kreves for å utstede en overvåkningsordre. Her henvises det til straffebestemmelser som ellers er tilgjengelige.

Artikkel 12 beskriver nærmere varigheten av overvåkning som er iverksatt i tråd med artikkel 5 (overvåkning på bakgrunn av straffeforfølgelse), artikkel 6 (overvåkning på bakgrunn av

---

[18] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf, se avsnitt 26 – 31

[19] Ibid, se avsnitt 26

[20] Ibid, se avsnitt 28

[21] Ibid, se avsnitt 29

[22] Ibid, se avsnitt 30

[23] Ibid, se avsnitt 31.

valgpåvirkning og trussel mot demokratiet) og artikkel 7 (overvåkning på bakgrunn av utenlandsk etterretning og spionasje). Begrensninger i de registrertes rettigheter beskrives gjennomgående i CSSA.

4.3.1.2. Garanti B: Nødvendig og proporsjonal for å oppnå et legitimt formål.

Artikkel 2 stiller krav om at eventuell overvåkning skal være nødvendig, forholdsmessig og formålstjenlig. Riktignok er det uklart hvordan dette begrenser det statlige handlingsrommet mer konkret. Tilsvarende formuleringer om nødvendighet, forholdsmessighet og formålstjenlighet er dessuten innlemmet i øvrige deler av lovverket der disse kravene er naturlig å fremheve.

4.3.1.3. Garanti C: Uavhengig tilsyn og kontroll (domstolskontroll)

Det finnes ikke et dedikert og uavhengig kontrollorgan opp mot håndhevingen av CSSA.

En «enforcement authority» skal etter artikkel 5 oversende minst en rapport til hver 15 dag underveis i gjennomføringen av kommunikasjonsovervåkning. Rapporten skal leveres til aktoren eller dommeren som utstedte bestillingen om overvåkning. Innholdet i rapporten skal inkludere status på progresjon samt en redegjørelse av om overvåkningen er nødvendig å videreføre.

Etter artikkel 16-1 skal «enforcement authority» og «supervisory authority» forberede en årlig rapport med relevant statistikk om det foregående årets overvåkningsaktivitet.

Det fremkommer videre av artikkel 32-1 at «The ministry of Justice» skal gjennomføre årlige revisjoner på «the status of the enforcement of communications surveillance.». Funnene skal videre rapporteres til «Legislative Yuan», som er et justisutvalg organisert under den taiwanske kongressen stemt frem via demokratiske valg. [24]

CSSA inneholder ingen beskrivelse av en uavhengig kontroll- og tilsynsmyndighet. Hertil er det også av betydning at det per nå, som nevnt i punkt 3.1.5, heller ikke eksisterer en dedikert, uavhengig og kontrollerende aktør tilsvarende europeiske datatilsyn etter PDPA. Senere endringer ved PDPA har imidlertid formalisert etableringen av et slikt organ. Dette organet skal kalles Personal Data Protection Comission (PDPC), men er enda ikke virksomt i praksis.[25] Ifølge lokal ekspertise ble det etablert et «preperatory office» for PDPC 5.desember 2023, og det antas at PDPC skal være virksomt innen august 2025.

National Development Council (NDC) skal håndheve og avsi beslutninger på saker på PDPAs område, samt kompetanse til å tolke både PDPA og de interne prosedyrene som statlige aktører er forpliktet til å etablere under PDPA.

4.3.1.4. Garanti D: Effektive rettsmidler

Tilstedeværelse av effektive rettsmidler forutsetter blant annet at de registrerte settes i stand til å gjøre sine rettigheter gjeldende. Om, og i hvilken grad de registrerte varsles om iverksatt eller gjennomført overvåkning er derfor av stor betydning, ifølge EDPB.

Artikkel 15 i CSSA beskriver myndighetenes ansvar for å varsle person(e) som overvåkes. Her følger blant annet at med mindre varsel om gjennomført overvåkning strider med det opprinnelige overvåkningsformålet, skal «The court» informere personen(e) som overvåkes innen 14 dager etter at overvåkningen er ferdig. Artikkel 15 beskriver også nærmere krav til innhold i et slikt varsel.

«The court» er ikke gitt noen nærmere beskrivelse i CSSA når det gjelder ansvarsområde, uavhengighet, kompetanse eller annet. En rimelig slutning er likevel at «the court» må være en

[24] https://en.wikipedia.org/wiki/Legislative_Yuan.
[25] Taiwan - Data Protection Overview | Guidance Note | DataGuidance, punkt 1.1, 3.1.

domstol eller annen kompetent autoritet med myndighet til å avsi beslutninger i strafferettslige saker ettersom hjemmelsgrunnlag for overvåkning etter CSSA i hovedsak forutsetter en kriminalisert handling etter den nasjonale strafferetten (se artikkel 5 og 7).

Ifølge EDPB stilles det ikke krav til at «the court» er en formell domstol. Så lenge saker kan føres for en «national authority» eller en «body» som tilbyr garantier nevnt i artikkel 47 i charteret, må dette være tilstrekkelig.[26] Av betydning er det også at det aktuelle organet er gitt myndighet til å avsi beslutninger som er bindende for den nasjonale overvåknings- og etterretningstjenesten. På dette punktet er det uklart «the court» er tillagt slik myndighet i Taiwan.

Når det gjelder bruken og fullbyrdingen av anvendelige rettsmidler, fremkommer det av artikkel 24 i CSSA at ulovlig overvåkning straffes med «fixed-term imprisonement» opp til fem år. Ulovlig lekkasje av hemmelig eller annen type informasjon innhentet i tråd med øvrige hjemler i CSSA, straffes også med «fixed-term imprisonment» i opptil fem år.

CSSA tilbyr ingen mulighet til umiddelbar håndhevingen av rettigheter eller bruk av rettsmidler dersom ulovlig overvåkning iverksettes. Dette skyldes at hemmelighold er en grunnleggende del av enhver overvåkningsaksjon, hvilket vanskeliggjør

Til sist kan det nevnes at PDPA tilrettelegger for både administrativ og juridisk prosess for registrerte som har fått sine data utlevert («transferred»).[27] Under visse omstendigheter gir PDPA «data subjects» rett til å protestere en behandling, gjennomgå, revidere, supplere eller slette personopplysninger om seg. Dette punktet er imidlertid kun relevant i den grad rettsmidlene nevnt i PDPA også kan gjøres gjeldene opp mot overvåkning med hjemmel i CSSA, hvilket er usikkert.

4.3.1.5. Delkonklusjon

Prosjektets vurdering er at CSSA ikke oppfyller de grunnleggende europeiske garantiene. Dette gjelder garanti C og D. Konsekvensene av dette er at prosjektet må vurdere behovet for ytterligere supplerende tiltak for å sikre tilstrekkelig beskyttelsesnivå for overføringen av personopplysninger.

4.4. Hvordan håndheves de relevante regelverkene i praksis

Prosjektet vurderer videre hvordan regelverkene som gjelder for overføringen gjennomføres i praksis.

Etter EDPBs veiledning kan en analyse av tredjelandets praksis bidra til å verifisere vurderingen av lovgivningen opp mot de grunnleggende garantiene. Ettersom CSSA ikke oppfyller de grunnleggende garantiene vil det i utgangspunktet ikke være nødvendig å trekke inn og vektlegge praksis på denne måten. Prosjektet velger likevel å inkludere en beskrivelse av praksis fordi praksis er relevant for å identifisere supplerende sikkerhetstiltak i neste steg i TIA-en.

Redegjørelsen under inneholder en gjennomgang av praksis fra PDPA, CSSA, Google, i tillegg til en gjennomgang av «Taiwan Internett Transparency Report» levert av Taiwan Association for Human Rights. Til sist følger en oppsummering av dialog med lokal ekspertise i Taiwan.

---

[26] Se https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf, avsnitt 46 og 47.

[27] Taiwan – Third Country Assessment | Guidance Note | DataGuidance, punkt 2.3.

4.4.1. Domstolspraksis

4.4.1.1. Domstolvesenet i Taiwan

«Judicial Yuan» er en gren av den sentrale statsforvaltningen og utgjør det statlige rettsapparatet med domstoler i Taiwan. Ansvaret for- og driften av den Taiwanske konstitusjonsdomstolen er dermed lagt til «Judicial Yuan», sammen med øvrige deler av det fungerende rettssystemet, herunder ordinære domstoler, ankedomstoler, distriktsdomstol, høyesterett m.m.

Konstitusjonsdomstolen består av 15 dommere utnevnt av presidenten i Taiwan. Dommerne kan ikke tre inn i embetet uten samtykke fra «Legislative Yuan», som er det lovgivende organ i Taiwan. Innsetting av konstitusjonsdommere synes å være gjenstand for kontroll både fra den lovgivende- og den utøvende makt. Utvelgelsesprosessen har dermed et visst politisk preg.

4.4.1.2. PDPA

Det finnes flere eksempler på domsbeslutninger som angår PDPA og tilgrensende lovverk i Taiwan. Dette er dommer avsagt av den øverste administrative domstolen («Supreme Administrativ Court»), ankedomstolen «Taiwan High Court», samt av «Taipei District Court».[28] Dommene gjelder i hovedsak håndheving og etterlevelse av rettighetene etter PDPA, og særlig avveiningen av disse rettighetene opp mot statlige interesser og hensyn.

Prosjektet kan ikke se at det finnes domsbeslutninger som angår PDPA og som det er relevante å drøfte i denne analysen. Grunnen til det er at PDPA, slik prosjektet ser det, ikke verner norske brukere av GWE som er lokalisert i Norge. Vi går derfor ikke nærmere inn på PDPA i denne landvurderingen.

4.4.1.3. Sak nr. 631.

Den Taiwanske konstitusjonsdomstolen har publisert en «interpretation» (heretter tolkning) kalt «Issuance of Communications Surveillance Warrants Case» (tolkning nr. 631 fra 2007). Konstitusjonsdomstolen er en del av det Taiwanske «Judicial Yuan». Tolkningen gjelder rettsanvendelsen i Criminal Judgement 92- Shang-Su-882 (2003) som ble avsagt i «Taiwan High Court».[29]

Tolkningen omhandler grunnlovmessigheten av artikkel 5 paragraf 2 i CSSA opp mot artikkel 12 i Taiwans grunnlov om «freedom of secrecy of correspondence», og vektes i Taiwan som et autoritativt tolkningsbidrag inn mot håndhevingen av regelverket, både for alminnelige rettsanvendere i Taiwan, men også for øvrige domstoler.

Saken gjaldt overvåkning av en telefonsamtale mellom en Taiwansk polititjenestemann og Ms. X, der polititjenestemannen på forespørsel fra Ms. X hadde utlevert informasjon om Ms. KAO fra påtalemyndighetens database. Utleveringen av informasjon var ulovlig etter taiwansk straffelov, men fordi politiordre om overvåkning etter artikkel 5 paragraf 2 i CSSA ikke krever godkjenning fra en kompetent domstol, anførte politioffiseren at overvåkningen av telefonsamtalen var i strid med artikkel 12 i den Taiwanske grunnloven. [30]

Under «Reasoning» beskriver domstolen nærmere hvilke hensyn og interesser som bør ivaretas i håndhevingen av CSSA. I omtalen av overvåkningsvirksomhet med hjemmel i artikkel 2, 5 og 7 i CSSA, understreker domstolen at «[c]ommunications surveillance is essentially a measure that violates the people's basic rights with extreme force and in a broad way. In order to achieve the purpose of the

[28] https://www.dataguidance.com/notes/taiwan-data-protection-overview, punkt 1.3.
[29] https://cons.judicial.gov.tw/en/docdata.aspx?fid=100&id=310812,
[30] Leading Cases of the Taiwan Constitutional Court, August 2018, Volume One, Judicial Yuan, No.631, «Background Note by the translator», s.111 – 119.

coercive measure, when conducting communications surveillance, the State usually deprives those who are put under surveillance of their rights to avoid such coercive measure before the measure is adopted.».

Videre fremhever domstolen viktigheten av å begrense «[…]unnecessary violations of privacy rights that occur due to the coercive measure adopted by investigation authorities and at the same time not compromise the purpose of the coercive measure.».

For å begrense graden av inngrep trekker domstolen frem nødvendigheten av å etablere «[…]an independent and impartial judicial institution in charge of reviewing government applications for communications surveillance warrants so that the people's freedom of secrecy of correspondence can be protected.».

Avslutningsvis legger domstolen til grunn at artikkel 5 paragraf 2 i CSSA, på daværende tidspunkt (2007), er i strid med retten til «secrecy of correspondence». Artikkel 5 paragraf 2 ble med dette ugyldiggjort.

Siden 2007 er det gjennomført flere lovendringer av artikkel 5 paragraf 2. Artikkelen inkluderer nå en formulering om at «[t]he interception warrant […] shall be applied for, during the investigation, by the prosecutor upon receiving applications from judicial police authoritites, or applied by the prosecutor ex officio to the **court** concerned for issuance.». Etter ordlyden kreves nå at søknad om politiordre for overvåkning skal rutes via og kontrolleres av «the court concerned for the issuance».

Dommen indikerer at det gjennomføres løpende vurderinger av grunnlovsmessigheten av hjemmelsgrunnlag for overvåkning. Tolkningen illustrerer at domstolen vekter inngrepets art og karakter opp mot etablerte rettsstatlige prinsipper om domstolskontroll og forholdsmessighet. Tolkningen resulterer i en lovendring som effektuerer en form for legalitetsprinsipp; graden av inngrep dikterer hvilke rettssikkerhetsmekanismer som implementeres. Lovverket fremstår også dynamisk ved at konkrete bestemmelser kan bli gjenstand for endring basert på rettsstatlige prinsipper/hensyn eller individuelle rettigheter.

4.4.2. Taiwan Internet Transparency Report

Taiwan Association for Human Rights ("**TAHR**") publiserte i 2015 en rapport kalt «Taiwan Internet Transparency Report» (heretter kalt "**TITR**" eller "**rapporten**"). Formålet med rapporten var blant annet å synliggjøre graden av inngrep i retten til privatliv og personvern i Taiwan. Rapporten er resultatet av et forskningsprosjekt gjennomført av TAHR. Funnene er hentet fra perioden 2012 til 2014. Selv om rapporten er fra 2015, er det grunn til å tro at tallene fremdeles er representative for situasjonen i Taiwan. Rapporten vurderes derfor til å være relevant for landvurderingen.

I rapporten vises det til at taiwanske myndigheter - særlig etter 2010, har vesentlig styrket landets teknologiske overvåkningsevner.[31] Dette har medført en betydelig økning i avlyttingvirksomhet i Taiwan. TAHR rapporterer videre at etterlevelsen av rettsstatsprinsippene om skjellig grunn til mistanke, rettferdig prosess, og uavhengig og kontrollerende tilsynsorgan mangler. Rapporten etterlyser økt gjennomsiktighet slik at saker kan bli prøvd for åpne domstoler. I den forbindelse fremhever hovedforfatter av rapporten, Ho Ming-syuan, at «[…]a great number of device users had not been informed about the surveillance demands and were left in the dark.», og legger videre til at

[31] https://globaltaiwan.org/2020/02/closing-loopholes-in-the-legal-framework-for-government-surveillance-in-taiwan/

«[…]most authorities simply skipped the legal procedures by writing to the operators, asking for information they wanted.». [32]

Rapporten fremlegger statistikk på begjæringer/forespørsler om utlevering av- eller innsyn i data sendt fra ulike statlige organer. Statistikken synliggjør hvilke konkrete lover og bestemmelser som begjæringene var hjemlet i. Her kommer det frem at en stor andel begjæringer er hjemlet i CSSA. Dette gjelder også på tvers av myndighetsområder (se Coast Guard Administration og National Police Agency). [33]

Rapporten kategoriserer også forespørsler om overvåkning på bakgrunn av formål. Under «Overview on reasons for internet personal data requests in 2012-2014», rapporteres det at i perioden 2012 til 2014 var 3765 av 4908 (76 %) forespørsler begrunnet i kriminaletterforskning. Tallene baserer seg på tilbakemeldinger fra kun syv av totalt 14 organer som ble forespurt deling av statistikk. Antallet totale forespørsler (4908) som er rapportert reflekterer derfor trolig ikke det fullstendige bilde av overvåkningsvirksomheten i Taiwan mellom 2012 og 2014.

Som nevnt i punkt 4.3.1.3 følger det videre av artikkel 16-1 i CSSA at «enforcement authority» og «supervisory authority» skal forberede en årlig rapport med relevant statistikk om det foregående årets overvåkningsaktivitet. I 2015 begjærte TITR-prosjektet innsyn i denne rapporten og «Department of Satistics of the Judicial Yuan» innvilget innsyn og tilgjengeliggjorde statistikk fra andre halvdel av 2014. Statistikken var inndelt i åtte kategorier (linjer) kommunikasjonsovervåkning;

1. Lokal telefon- og mobilovervåkning,
2. IMEI («International Mobile Equipment Identity»),
3. IMSI («International Mobile Subcscriber Identity»),
4. HiNet ADSL-kontoer,
5. Internettelefonkonto (f.eks. Skype),
6. Epostadresser,
7. IP-adresser,
8. Annet,

I løpet av andre halvdel av 2014 ble det oversendt 14292 forespørsler om kommunikasjonsovervåkning på tvers av 21125 linjer. Av totalt 14292 forespørsler gjaldt 89,31% (12841) av disse overvåkning av lokalt telefon- og mobilnettverk.[34]

Statistikken er mangelfull på flere områder. Ifølge rapporten regnes det med betydelige mørketall. Når statistikk fra Judicial Yuan sammenlignes med statistikk tilgjengeliggjort eller oversendt fra organisasjoner som har mottatt forespørsler om innsyn eller utlevering av data, avdekkes vesentlige uoverensstemmelser. Rapporten belyser flere forhold og omstendigheter som kan være utslagsgivende i denne sammenheng;

- **Mangel på konkrete tall:** Av 14 myndighetsorgan i Taiwan som ble forespurt deling av informasjon var det bare 7 som svarte.
- **Manglende retningslinjer og prosedyrer:** Ifølge rapporten var det bare «Criminal Investigation Bureau» som kunne bekrefte at det var etablert prosedyrer for å systematisere

[32] Taiwan Internet Transparency Report, a research project on internet freedom and online privacy conducted investigate and track the personal data requests and content removal request situation done by government units, Taiwan Association for Human Rights (TAHR), https://transparency.tahr.org.tw/TITR_Report_2015_en.pdf.
[33] Ibid, side 10 og 11.
[34] Ibid, side 27

tall på egen virksomhet. Det kan dermed sluttes at mangel på klare retningslinjer og prosedyrer for føring av statistikk ved de enkelte myndighetsorganene er en gjentakende utfordring.[35]

- **Manglende samarbeidsvillighet:** Flere organer unnlot å svare eller motsatte seg forespørsel fra TAHR om deling av statistikk.[36]
- **Ulik forståelse og perspektiv:** Det synes å foreligge store forskjeller i definisjonen av en personopplysning på tvers av aktørene som TAHR har vært i kontakt med.
- **Rettslig munnkurv:** Ifølge National Security Bureau i Taiwan er organet rettslig forhindret å dele informasjon etter artikkel 16-1 paragraf 2 i CSSA. Denne type «munnkurv» gjelder trolig også flere andre aktører.[37]

4.4.2.1. Slutning fra «Taiwan Internet Transparancy Report(TITR)»

Rapporten avdekker en rekke forhold som er relevant for vurderingen av hvordan CSSA gjennomføres i praksis. Det er likevel to punkter som etter prosjektets vurdering er særlig viktig for å vurdere betydningen for vernet av personopplysninger som overføres til Taiwan:

1) Ifølge rapporten gjaldt 89 % av rapporterte overvåkningsforespørsler lokalt telefon- og mobilnettverk. Ettersom bruk av GWE i norske skoler kun involverer databehandling i de øvrige tjenestenivåene i OSI-modellen, kan det argumenteres for at gjennomføringen av CSSA, i praksis, i liten grad dekker overføringen til Taiwan.

2) Ifølge rapporten ble 76 % av alle overvåkningsforespørsler mellom 2012 og 2014 gjennomført som ledd i en kriminaletterforskning. Prosjektet trekker følgende konklusjon av dette: I den grad overvåkning i Taiwan forekommer, vil overvåkningen med overveiende sannsynlighet være utløst av taiwanske straffebestemmelser. Dette innebærer en betydelig innsnevring av hvilke data som kan bli berørt av statlig overvåkning med hjemmel i CSSA.

4.4.3. Google

4.4.3.1. Googles «Transparency Reports»

Google offentliggjør løpende rapporter med statistikk på globale forespørsler om brukerinformasjon. Rapportene oppdateres hver sjette måned. Her deles antall og type forespørsler som Google mottar fra offentlige myndigheter.[38]

Siden januar 2020 og frem til 2024, rapporterer Google om totalt 5550 forespørsler fra Taiwanske myndigheter. I gjennomsnitt er litt over halvparten av forespørslene fulgt opp med utlevering av data. I rapportene skilles det mellom «Emergency disclosure requests», og «Other legal requests». Det er ikke kjent hva to-delingen gjelder, eller hvilke lover som forespørslene er hjemlet i. Rapporten tilfører kun et kvantitativt overblikk over situasjonen fra Googles side.

4.4.3.2. Korrespondanse med Google

Prosjektet har tatt kontakt med Google og etterspurt deling av informasjon relevant for landvurderingen. Vi sendte en skriftlig forespørsel til Google 29. april 2024 og fikk svar 10. mai 2024. I

[35] Ibid, side26
[36] Ibid, side 25
[37] Ibid, side 24
[38] https://transparencyreport.google.com/user-data/overview?hl=en_US&user_requests_report_period=series:requests,accounts;authority:TW;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0

forespørselen ble Google anmodet om å svare ut/beskrive Googles håndtering av utleveringsforespørsler fra taiwanske myndigheter.

Prosjektet vurderer svaret fra Google til å ha begrenset verdi for landvurderingen. Google henviste til allerede offentlig tilgjengelig informasjon i deres «Transparency Reports». Det var kun Googles rapportering av statistikk for utleveringsbegjæringer knyttet GWE som var av betydning for prosjektet. Google melder at det kun var mottatt 4 forespørsler knyttet GWE i 2022. I lys av rapporten fra TAHR under punkt 4.4.2.1 (1), tyder dette på liten til ingen endring i hyppighet og omfang av overvåkning siden 2014. Det er liten grunn til å tro at situasjonen vil endres kommende år.

4.4.4. Lokal ekspertise i Taiwan

Prosjektet har vært i dialog med lokal ekspertise i Taiwan og har i den forbindelse oversendt spørsmål til advokatfirmaet Nishimura & Asahi Taiwan. Hensikten er å verifisere at prosjektets tolkning av Taiwansk lovgivning stemmer overens med gjeldende rett i Taiwan. Spørsmålene inneholder påstander om Taiwansk lovgivning som vi har hatt behov for å få bekreftet/avkreftet.

Nishimura & Asahi støtter prosjektets konklusjoner på sentrale punkter. Svar fra Nishimura & Asahi Taiwan sammen med våre spørsmål kan finnes i vedlegg til denne landvurderingen.

4.5. Oppsummering av praksis

Gjennomgangen av praksis gir en forståelse av hvordan relevante regelverk for dataoverføring håndheves i Taiwan. Prosjektet følger veiledningen fra EDPB, som anbefaler analyse av tredjelandets praksis for å verifisere lovgivningens oppfyllelse av grunnleggende garantier. Selv om CSSA ikke oppfyller disse garantiene, inkluderes en praksisbeskrivelse for å identifisere supplerende sikkerhetstiltak i TIA-analysen.

Teksten gir en detaljert gjennomgang av domstolspraksis, herunder beskrivelse av «Judicial Yuan» og en sak (tolkning nr. 631) som gjelder lovlighet av overvåkning under CSSA. Denne tolkningen resulterte i at en lovparagraf ble funnet grunnlovsstridig og senere endret for å inkludere domstolskontroll ved overvåkningsforespørsler.

Videre gjennomgås «Taiwan Internet Transparency Report» (TITR) fra 2015, som viser økt overvåkningsvirksomhet og manglende rettsstatsprinsipper i Taiwan. Rapporten peker på betydelige mørketall og manglende åpenhet fra taiwanske myndigheter.

Googles «Transparency Reports» viser at det har vært relativt få forespørsler om utlevering av data fra taiwanske myndigheter. Prosjektet har også korrespondert med Google, som bekreftet begrenset antall forespørsler knyttet til GWE.

5. Konklusjon og anbefaling

Landvurderingen viser at selv om lovverket og praksisen i Taiwan har blitt endret for å øke rettssikkerheten, er det fortsatt betydelige utfordringer med hensyn til overvåkning og gjennomsiktighet. Spesielt fremheves det at de fleste overvåkningsforespørsler er relatert til kriminaletterforskning og i stor grad påvirker lokal telefoni og mobilnettverk.

Dette kan indikere at bruk av GWE i norske skoler sannsynligvis ikke vil bli sterkt berørt av taiwansk overvåkning. Likevel er det usikkerhet rundt den fulle graden av myndighetenes inngrep i personvern og privatliv, noe som krever at man iverksetter supplerende sikkerhetstiltak.

Basert på analysen over frarådes det å overføre personopplysninger til Taiwan. Dette er på grunn av de betydelige bekymringene rundt håndhevingen av CSSA i praksis og mangelen på garantier for personvern.

Det er viktig å merke seg at dette bare er en anbefaling, og at den endelige beslutningen om hvorvidt man skal overføre personopplysninger til Taiwan må tas av den enkelte organisasjon basert på sin egen vurdering av risikoen.

Litteraturliste

Lovverk og annen rettslig dokumentasjon

Personal Data Protection Act (PDPA), https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021

Telecommunications Act (TA), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060001

Telecommunications Management Act (TMA), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060111

European Data Protection Board (EDPB), «Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020», 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

Constitutional Court R.O.C (Taiwan), No.631 [Issuance of Communications Surveillance Warrants Case], 20.07.2007, https://cons.judicial.gov.tw/en/docdata.aspx?fid=100&id=310812

Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven), artikkel 8, https://lovdata.no/dokument/NL/lov/1999-05-21-30/KAPITTEL_2#KAPITTEL_2

Litteratur

31 J. Marshall J. Info. Tech. & Privacy L. 145, «Eyes on the Road Program in Taiwan—Information Privacy issues under the Taiwan Personal Data Protection Act», 2015, https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1758&context=jitpl

Leading Cases of the Taiwan Constitutional Court, «Background Note by the translator, No.631, Volume One, Judicial Yuan, 2018,

Øvrig kilder

DataGuidance Taiwan - Data Protection Overview | Guidance Note | DataGuidance

Freedom House, Taiwan Overview, https://freedomhouse.org/country/taiwan/freedom-net/2021

Global Taiwan Institute, Closing Loopholes in the Legal Framework for Government Surveillance in Taiwan, Global Taiwan Brief, Vol. 5, Issue 3, 2020, https://globaltaiwan.org/2020/02/closing-loopholes-in-the-legal-framework-for-government-surveillance-in-taiwan/

Legislative Yuan, https://en.wikipedia.org/wiki/Legislative_Yuan

Lee and Li, Attorneys at Law, Newsletter, «The Telecommunications Management Act Becomes Effective on July 1, 2020», https://www.leeandli.com/EN/NewslettersDetail/6496.htm

Taiwan Internet Transparency Report, Taiwan Association for Human Rights (TAHR), 2015, https://transparency.tahr.org.tw/TITR_Report_2015_en.pdf

Google Transparency Report, Global requests for user information, Taiwan, https://transparencyreport.google.com/user-data/overview?hl=en_US&user_requests_report_period=series:requests,accounts;authority:TW;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0

Illustrasjoner

OSI Model, https://cdn.codegym.cc/images/article/3effcdd0-5b89-4574-b154-c2c1c65d945d/512.jpeg

Spørsmål og svar fra lokal ekspertise ved advokatfirmaet Nishimura & Asahi Taiwan

#	Question	Response (Yes or No)	Brief explanation (please include reference to source)	Likelihood of enforcement (Low Medium or High)	Further comments (if any)
1	Is KS' preliminary assessment of what Taiwanese legislation applies to the data transfer as set out above correct and complete? If not, please describe any other laws or regulations that might apply to the data transfer.	No	• According to Paragraph 2, Article 51 of the PDPA, and the explanation promulgated by the competent authority (Fa-Lu-Zi No. 10403509750 dated 26 August 2015), **the PDPA applies to all collection, processing, and use of personal data occurring within the territory of Taiwan**, regardless of whether the data subject in question is located within Taiwan or not. • Furthermore, "processing" in the PDPA refers to the act of recording, inputting, **storing**, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, connecting, or internally transferring data for the purpose of establishing or using a personal data file, and "use" refers to the act of **using personal data via any methods** other than processing. (Article 2 of the PDPA). • As such, in this case, through using GWE, Norwegian users' personal data may be transferred and stored in data centres located in Taiwan and may be retransferred back to the EU/EEA from Taiwan. This constitutes processing and use of personal data within the territory of Taiwan,	High	

			to which the PDPA shall apply. • In addition, Paragraph 2, Article 51 of the PDPA stipulates that the PDPA also applies where an entity collects, processes, or uses the personal data of Taiwan nationals outside the territory of Taiwan. It cannot be ruled out that such "entity" may include a foreign entity established or organised in any other country than Taiwan. Therefore, even if the processing occurs outside Taiwan, if the personal data processed through GWE includes data of Taiwan nationals (e.g., Taiwanese nationals residing in Norway), the PDPA may still apply.		
2	Is there other general or sector-specific legislation that impacts data protection in the context of education or technology sectors, e.g. for datacenter, server and storage services for personal data?	-	• Apart from the legislations mentioned in the RFQ, regulations authorised by Article 27 of the PDPA oblige certain data holders to implement security measures to safeguard personal data. For example, according to "Regulations on the Personal Data Security Maintenance and Management in Digital Economy Related Industries" (數位經濟相關產業個人資料檔案安全維護管理辦法), which are applicable to data centres, servers, storage services, and relevant industries, managers of such facilities shall implement internal control protocol, among other security measures, to safeguard personal data (please refer to item 8 hereunder). • Articles 347 of the "Code of Civil Procedure" (民事訴	High Low	

			訟法) stipulates that the court may order, by a ruling, a third person to submit documents and data in its possession. • Article 47 of the "Law Governing the Legislative Yuan's Power" (立法院職權行使法), which came into force on 26 June 2024, provides that investigative committees assembled in the Legislative Yuan, which is the legislative body of Taiwan, may demand individuals or enterprises to provide documents and data related to their investigations. Data protection may be impacted in the highly unlikely event that Google is requested to submit or provide relevant data in accordance with above laws.		
3	Please consult our assessment of the CSSA above. Is our summary and assessment of the Act accurate based on the context provided by us and your understanding of the data that is stored in Taiwan and the GWE service? In particular, please advise of any independent control bodies.	No	• The CSSA governs communication surveillance conducted for the purposes of criminal investigation and national security. As it cannot be ruled out that Norwegian users of GWE may involve individuals or entities that fall into the definition of "foreign forces" in Article 8, or may be the subject of criminal investigation, the GWE service and relevant data is subject to the CSSA. • However, according to a precedent (最高法院106年度台非字第259號判決) of the Supreme Court of Taiwan, which has a de facto binding effect on courts, the CSSA applies to contents of **ongoing communications and**	Low	

			data of communication records (as defined in Paragraph 1 of Article 3-1, which means telecommunications numbers of the sender and the recipient, time of communication, length of use, address, service type, and mailbox or location information generated by the telecommunications system after the telecommunications user uses the telecommunications services) **and user information** (as defined in Paragraph 2 of Article 3-1, which means the telecommunications user's name, identification document number, telecommunications number, and information in the application, for any type of telecommunications service), but not to other data. A search warrant issued in accordance with Article 122 and 128 of the Code of Criminal Procedure will be required to access other data stored in data centres. • Given its purposes of criminal investigation and national security, the competent authorities of the CSSA are courts, prosecutors' offices, and the National Security Bureau. However, there is no independent control body specific to the CSSA. An independent data protection authority is being established in Taiwan (please refer to item 6 hereunder). • Since communication surveillance is of a covert nature, no immediate relief is provided in the CSSA, however,		

			ex post remedy is available according to Article 19; court decisions are binding for national surveillance and intelligence services.		
4	Has the Telecommunications Management Act fully replaced the Telecommunications Act in Taiwan?	Yes	The TMA entered into force on 1 July 2020, and had a three-year transition period which ended on 30 June 2023. The TA remains in effect but serves only as the legal basis of certain statutory fee charges and has become irrelevant to data protection and other regulatory matters. The TMA has fully replaced the TA in this regard.	N/A	
5	Does Google as a SaaS provider fall within the scope of Taiwanese telecom legislation? Please elaborate on potential consequences for the data subjects' privacy rights.	Yes	It is correct that "telecommunications services" defined in the TA and TMA are limited to public communications services provided through the public switched telecommunications network ("PSTN") and therefore Google as a SaaS provider does not fall within the scope of the TA and TMA.	N/A	
6	Are any significant changes to applicable legislation expected? If possible, please indicate when these changes will come into force.	-	• Regarding the PDPA, there is a significant legislative change expected as follows. • Currently, Taiwan does not have an independent data protection authority under the PDPA. Nevertheless, a recent amendment to the PDPA, dated 16 May 2023, designates the new Personal Data Protection Commission ("PDPC") as the independent competent authority for personal data protection (Article 1-1 of the PDPA). Article 1-1 of the PDPA has not been enacted yet, as the PDPC has not been established at the present time. The preparatory office for the PDPC was established on 5 December 2023, and recent news reports suggest that the PDPC is expected to be established by August 2025.	N/A	

7	Is a foreign data subject able to enforce their prescribed privacy rights in the jurisdiction under prescribed law, if relevant? Please also indicate any perceived express hinderances in law, regulation or case law to such data privacy rights enforcement.	-	• In the event that a data subject, whether Taiwanese or foreign, has its personal data collected, processed, or used within the territory of Taiwan, the PDPA will apply. As such, the data subject may then enforce the privacy rights provided by the PDPA in that jurisdiction. • In addition, the prescribed privacy rights under the PDPA are as follows: (i) the right to make an inquiry regarding and to review his/her personal data; (ii) the right to request a copy of his/her personal data; (iii) the right to supplement or correct his/her personal data; (iv) the right to demand the cessation of the collection, processing, or use of his/her personal data; and (v) the right to erase his/her personal data. Article 3 of the PDPA also provides that such rights shall not be waived or limited contractually in advance, so there are no express hindrances to such data privacy rights enforcement under the PDPA.	N/A	
8	Is there any security measures assumed to be effective for protection of data processed in Taiwan? Please provide a brief overview of industry standards of data security provided in the region, if available.	-	• In reference to item 2 above, the "Regulations on the Personal Data Security Maintenance and Management in Digital Economy Related Industries" (數位經濟相關產業個人資料檔案安全維護管理辦法) require data centres, servers, storage services, and relevant industries to implement security measures to safeguard personal data files. The security measures provided therein are assumed to be effective for the protection of data	N/A	

			processed in Taiwan. In addition, these regulations may apply to data centres located in Taiwan, including Google data centres storing Norwegian personal data in this regard. • These regulations provide an industry standard requiring data centres and relevant industries located in Taiwan to implement proper security measures to prevent personal data from being stolen, altered, damaged, destroyed, or disclosed as follows. (1) allocating management personnel and reasonable resources; (2) defining the scope of personal data; (3) establishing a mechanism of risk assessment and management of personal data; (4) establishing a mechanism of preventing, giving notice of, and responding to a data breach; (5) establishing an internal control procedure for the collection, processing, and use of personal data; (6) confirming restrictions on cross-border transfers, providing notice to data subjects, and supervising; (7) managing data security and personnel; (8) promoting awareness, education, and training; (9) managing facility security; (10) establishing an audit mechanism of data security; (11) keeping records, log files, and relevant evidence;		

			and (12) implementing integrated and persistent improvements on the security and maintenance of personal data.		