



Udtalelse 28/2025 om Europa- Kommissionens udkast til genne8mførelsesafgørelse i henhold til forordning (EU) 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Brasilien

Udgave 1.0

Vedtaget den 04 November 2025

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Resumé

Den 5. september 2025 indledte Kommissionen processen hen imod vedtagelsen af sit udkast til gennemførelsesafgørelse ("udkast til afgørelse") om tilstrækkelig beskyttelse af personoplysninger i Den Føderative Republik Brasilien ("Brasilien").

Den 5. september 2025 anmodede Kommissionen om en udtalelse fra Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet"). Databeskyttelsesrådets vurdering af tilstrækkeligheden af det beskyttelsesniveau, som Brasilien yder, er foretaget på grundlag af en undersøgelse af selve udkastet til afgørelse samt på grundlag af en analyse af den dokumentation, der er offentligt tilgængelig på de brasilianske myndigheders officielle websteder.

Databeskyttelsesrådet fokuserede på vurderingen af både de generelle aspekter af databeskyttelsesforordningen i udkastet til afgørelse og på offentlige myndigheders adgang til personoplysninger, der overføres fra EØS med henblik på retshåndhævelse og national sikkerhed, herunder de retsmidler, der er til rådighed for personer i EØS. Databeskyttelsesrådet vurderede også, om de garantier, der er fastsat i den retlige ramme i Brasilien, er til stede og effektive.

Databeskyttelsesrådet har som hovedreference for dette arbejde anvendt referencen vedrørende et tilstrækkeligt beskyttelsesniveau, der blev vedtaget den 28. november 2017 af Artikel 29-Gruppen² og senest revideret og vedtaget den 6. februar 2018 af Databeskyttelsesrådet ("referencen vedrørende et tilstrækkeligt beskyttelsesniveau"), samt Databeskyttelsesrådets henstilling 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger.

Databeskyttelsesrådet noterer sig med tilfredshed, at databeskyttelsesrammen, navnlig den generelle databeskyttelseslov i Brasilien ("LGPD"), sammen med præsidentielle dekreter og bindende forskrifter udstedt af Brasiliens databeskyttelsesmyndighed (Agencia Nacional de Proteção de Dados, "ANPD"), fastsætter krav (herunder med hensyn til principper, registreredes rettigheder, overførsler, tilsyn og klage- og prøvelsesmuligheder), der ligger tæt op ad databeskyttelsesforordningen og Den Europæiske Unions Domstols ("EU-Domstolen") praksis.

Databeskyttelsesrådet konkluderede også, at Kommissionen i udkastet til afgørelse bør præcisere visse aspekter af Brasiliens retlige rammer og nøje overvåge udviklingen deraf.

Med hensyn til ansvarlighedsprincippet og kravene til konsekvensanalysen vedrørende databeskyttelse anser Databeskyttelsesrådet det for vigtigt, at der er en forpligtelse til at gennemføre den i tilfælde, hvor behandlingen kan medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og at konsekvensanalysen vedrørende databeskyttelse omfatter vurderingen af behandlingens nødvendighed og proportionalitet.

¹ Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF.

² Artikel 29-Gruppen, WP 254 rev.01, vedtaget den 28. november 2017 og senest revideret og vedtaget den 6. februar 2018, godkendt af Databeskyttelsesrådet.

Databeskyttelsesrådet opfordrer derfor Kommissionen til at overvåge den praktiske gennemførelse af disse krav.

LGPD fastsætter en begrænsning af videregivelsen af oplysninger til de registrerede eller tilsynsmyndigheden på grundlag af "forretnings- og fabrikshemmeligheder" i visse tilfælde. I betragtning af betydningen af gennemsigtighedskrav for de registreredes mulighed for at kontrollere, hvordan deres oplysninger behandles, samt betydningen af forpligtelserne til at samarbejde med tilsynsmyndigheden, navnlig for at give de oplysninger, der er nødvendige for dens tilsynsopgaver, opfordrer Databeskyttelsesrådet Kommissionen til at overvåge gennemførelsen af disse begrænsninger i praksis for bedre at forstå deres indvirkning på retten til information og adgang samt på ANPD's eventuelle beføjelser.

Med hensyn til reglerne om videreoverførsel opfordrer Databeskyttelsesrådet Kommissionen til at præcisere i udkastet til afgørelse, om overførsler kun kan gennemføres i overensstemmelse med betingelser, der svarer til artikel 49 i databeskyttelsesforordningen, og kun i de ekstraordinære tilfælde, hvor andre overførselsinstrumenter ikke kan anvendes. Kommissionen opfordres også til at præcisere, om de registrerede informeres om: mulige risici ved overførslen, når denne er baseret på deres samtykke, og omstændighederne ved overførslen (varighed og formål med overførslen, bestemmelseslandene, de involverede parter ansvar, de registreredes rettigheder og måder at udøve dem på), uanset hvilket overførselsværktøj der anvendes.

Endvidere opfordrer Databeskyttelsesrådet Kommissionen til at redegøre nærmere for opgaverne for det nationale råd for beskyttelse af personoplysninger og privatlivets fred samt dets samspil med ANPD.

For så vidt angår brasilianske offentlige myndigheders adgang til og brug af personoplysninger, der overføres til dataansvarlige og databehandlere i Brasilien med henblik på strafferetlig håndhævelse og nationale sikkerhedsformål ("myndighedsadgang"), bemærker Databeskyttelsesrådet, at LGPD ikke finder anvendelse på databehandling, der foretages udelukkende af hensyn til den offentlige sikkerhed, det nationale forsvar, statens sikkerhed eller efterforskning og retsforfølgning af strafbare handlinger. Samtidig bemærker Databeskyttelsesrådet på den positive side, at Brasiliens føderale højesteret i sin praksis har fortolket LGPD på en måde, der udvidede dens delvise anvendelse til behandling af personoplysninger med henblik på strafferetlig efterforskning og opretholdelse af den offentlige orden.

I lyset heraf opfordrer det Kommissionen til i udkastet til afgørelse yderligere at vurdere og præcisere anvendelsen af LGPD i tilfælde af behandling af personoplysninger med henblik på strafferetlig håndhævelse, herunder ANPD's undersøgelsesbeføjelser og korrigerende beføjelser over for retshåndhævende myndigheder, samt til nøje at tage hensyn til enhver relevant udvikling i denne henseende som led i sin overvågningsforpligtelse.

I betragtning af, at staterne har en bred skønsmargen til at definere spørgsmål om national sikkerhed, hvilket giver mulighed for undtagelser vedrørende national sikkerhed i forbindelse med behandling af personoplysninger, opfordrer Databeskyttelsesrådet Kommissionen til i udkastet til afgørelse at beskrive og forklare rammerne for begrebet national sikkerhed efter brasiliansk ret mere præcist. I den forbindelse opfordrer Databeskyttelsesrådet Kommissionen til yderligere at afklare, hvordan undtagelser fra LGPD af hensyn til national sikkerhed forholder sig til indsamling og deling af data mellem de offentlige enheder i det brasilianske efterretningssystem (SISBIN).

Indholdsfortegnelse

1. INDLEDNING	5
2. GENERELLE DATABESKYTTELSESASPEKTER	6
2.1 Ansvarlighed og datastyring	6
2.2 Anvendelsesområde og definitioner	7
2.2.1 LGPD's materielle og territoriale anvendelsesområde	7
2.2.2 Definitioner	8
2.3 Databeskyttelsesprincipper og retsgrundlag	8
2.3.1 Principper for behandlingen	8
2.3.2 Sikkerhedsforanstaltninger og -brud	10
2.3.3 Lovlig behandling	11
2.4 Individuelle rettigheder	11
2.5 Begrænsninger for videreoverførsel	12
2.6 Procedure- og håndhævelsesmekanismer	14
2.6.1 Uafhængigt tilsyn	14
2.6.2 Klagemuligheder	15
2.6.3 Sanktioner	15
3. BRASILIANSE OFFENTLIGE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT FRA DEN EUROPÆISKE UNION	16
3.1 Brasilianske offentlige myndigheders adgang til og anvendelse af oplysninger med henblik på strafferetlig håndhævelse	17
3.1.1 Retlige rammer for strafferetlig håndhævelse	17
3.1.2 Nødvendighed og proportionalitet	18
3.1.3 Videre anvendelse af data og videreoverførsler	19
3.1.4 Tilsyn og klagemuligheder	20
3.2 De brasilianske offentlige myndigheders adgang til og brug af personoplysninger til nationale sikkerhedsformål	21
3.2.1 Anvendelsesområdet for undtagelsen i artikel 4, nr. III, i LGPD og dens anvendelse på strafbare handlinger mod statens sikkerhed	22
3.2.2 Retsgrundlag for national sikkerhed	22
3.2.3 Videreoverførsler og internationale aftaler	24
3.2.4 Tilsyn og klagemuligheder	25
4. GENNEMFØRELSE OG OVERVÅGNING AF UDKASTET TIL AFGØRELSE	26

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra s), i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF ("databeskyttelsesforordningen"),

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde ("EØS-aftalen"), særlig bilag XI og protokol 37 som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg den 6. juli 2018³,

under henvisning til artikel 12 og artikel 22 i Databeskyttelsesrådets forretningsorden —

VEDTAGET FØLGENDE UDTALELSE:

³ Henvisninger til "medlemsstater" i denne udtalelse skal forstås som henvisninger til "EØS-medlemsstater".

1. INDLEDNING

- (1) Kapitel V i databeskyttelsesforordningen fastsætter betingelserne for overførsel af personoplysninger til et tredjeland eller en international organisation. Overførsel af personoplysninger kan finde sted på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet truffet af Kommissionen (artikel 45 i databeskyttelsesforordningen), eller, i mangel af en sådan afgørelse, hvis den dataansvarlige eller databehandleren giver de fornødne garantier, herunder rettigheder, som kan håndhæves, og retsmidler for den registrerede (artikel 46 i databeskyttelsesforordningen). I mangel af enten en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller fornødne garantier må en overførsel eller en række overførsler til et tredjeland eller en international organisation kun finde sted under visse betingelser (artikel 49 i databeskyttelsesforordningen).
- (2) Databeskyttelsesrådet minder om, at afgørelser om tilstrækkeligheden af beskyttelsesniveauet anerkender den fortsatte beskyttelse af personoplysninger, der overføres fra EØS til tredjelande eller internationale organisationer, og er et robust overførselsværktøj til at sikre, at den registreredes rettigheder beskyttes, når oplysninger overføres uden for EØS. I henhold til referencen vedrørende et tilstrækkeligt beskyttelsesniveau⁴ og til EU-Domstolens relevante praksis⁵ gælder det, at selv om tredjelandet ikke skal sikre et beskyttelsesniveau, der er identisk med det, der er sikret i Unionens retsorden, skal udtrykket "tilstrækkeligt beskyttelsesniveau" i databeskyttelsesforordningens artikel 45, stk. 1, forstås således, at det kræver, at dette tredjeland på grundlag af sin nationale lovgivning eller sine internationale forpligtelser faktisk sikrer et beskyttelsesniveau for de grundlæggende rettigheder og frihedsrettigheder, der i det væsentlige svarer til det, der er sikret i Unionen, sammenholdt med chartret om grundlæggende rettigheder.
- (3) Brasilien er en føderativ republik, der består af en union af 26 stater og et føderalt distrikt, som fastsat i landets forfatning ("forfatningen")⁶. De brasilianske stater har også deres egne forfatninger, som ikke må være i strid med den føderale forfatning. Privatlivets fred og databeskyttelse er beskyttet i forfatningen som grundlæggende rettigheder (forfatningens artikel 5, nr. X, XII og LXXIX)⁷ og anerkendt af forfatningsdomstolen for enhver person, herunder udlændinge, uanset om vedkommende er bosiddende i Brasilien⁸ eller ej.
- (4) Den vigtigste lovgivning om databeskyttelse er den generelle databeskyttelseslov eller "Lei Geral de Proteção de Dados" ("LGPD") (nr. 13.709 af 14. august 2018, senest ændret ved lov nr. 14.460 af 25. oktober 2022). LGPD suppleres af de bindende dekretter (præsidentdekret nr. 10.474 af 26. august 2020 og præsidentdekret nr. 11.758 af 30. oktober 2023), som er retligt bindende og kan håndhæves⁹.
- (5) Ud over LGPD omfatter den brasilianske databeskyttelsesramme bindende regler udstedt af Brasiliens databeskyttelsesmyndighed (Agencia Nacional de Proteção de Dados, "ANPD")¹⁰.

⁴ Artikel 29-Gruppen, WP 254 rev.01, vedtaget den 28. november 2017 og senest revideret og vedtaget den 6. februar 2018, godkendt af Databeskyttelsesrådet, kapitel 3, C.

⁵ EU-Domstolen, 6. oktober 2015, dom i sag C-362/14, Maximilian Schrems mod Data Protection Commissioner, ("Schrems") og Retten, 3. september 2025, dom i sag T-553/23, Philippe Latombe mod Europa-Kommissionen, ("Latombe").

⁶ Se betragtning 7 i udkastet til afgørelse.

⁷ Se betragtning 8 i udkastet til afgørelse.

⁸ Se betragtning 9 i udkastet til afgørelse.

⁹ Se betragtning 11 og 12 i udkastet til afgørelse.

¹⁰ Alle bindende forskrifter udstedt af ANPD findes her: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd.

Disse regler indeholder yderligere bestemmelser om fortolkningen og anvendelsen af LGPD¹¹. For eksempel forordning nr. 4 af 24. februar 2024 om anvendelse af administrative sanktioner, forordning nr. 15 af 24. april 2024 om underretning om sikkerhedshændelser, forordning nr. 19 af 23. august 2024 om international overførsel af personoplysninger ("dataoverførselsforordningen"), forordning nr. 2 af 27. januar 2022 om anvendelse af LGPD på små og mellemstore virksomheder og forordning nr. 18 af 15. juli 2024 om databeskyttelsesrådgiverens rolle ("databeskyttelsesrådgiverforordningen").

- (6) Databeskyttelsesrådet glæder sig over den forfatningsmæssige anerkendelse af retten til privatlivets fred og retten til databeskyttelse som grundlæggende rettigheder, der yderligere gennemføres via national lovgivning. Desuden noterer Databeskyttelsesrådet sig med tilfredshed de internationale forpligtelser, som Brasilien har påtaget sig¹².
- (7) Databeskyttelsesrådet bemærker, at Den Europæiske Unions institutioner¹³, organer, kontorer og agenturer i henhold til artikel 47 og 94 i forordning (EU) 2018/1725 kan overføre personoplysninger til et tredjeland, et område, en sektor eller en international organisation, hvis Kommissionen i henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 har fastslået, at de sikrer et tilstrækkeligt beskyttelsesniveau, forudsat, at oplysningerne kun overføres, for at der kan udføres opgaver, som henhører under den dataansvarliges kompetence, uden at kræve yderligere tilladelse. Databeskyttelsesrådet opfordrer Kommissionen til at minde om denne retlige mulighed i betragtningerne til udkastet til afgørelse.

2. GENERELLE DATABESKYTTELSESASPEKTER

2.1 Ansvarlighed og datastyring

- (8) I LGPD fastsættes princippet om ansvarlighed som et af de generelle principper for behandling af personoplysninger. Ifølge denne skal dataansvarlige og databehandlere¹⁴ vedtage passende tekniske og organisatoriske foranstaltninger til effektivt at overholde deres databeskyttelsesforpligtelser, og de skal kunne påvise en sådan overholdelse, bl.a. over for den kompetente tilsynsmyndighed (artikel 46 i LGPD). Databeskyttelsesrådet bemærker, at sådanne foranstaltninger omfatter udpegelse af en databeskyttelsesansvarlig (artikel 41 i LGPD), som nærmere beskrevet i ANPD's databeskyttelsesrådgiverforordning, konsekvensanalysen vedrørende databeskyttelse (artikel 38 i LGPD) samt føring af fortegnelser over databehandlingsaktiviteter (artikel 37 i LGPD). Desuden fastslår LGPD, at dataansvarlige og databehandlere kan formulere interne regler for god praksis og forvaltningsmodeller, herunder planer for uddannelsesaktiviteter, interne tilsynsmekanismer og risikobegrænsning (artikel 50 i LGPD). Databeskyttelsesrådet noterer sig med tilfredshed, at sådanne instrumenter svarer til dem, der er fastsat i databeskyttelsesforordningen til gennemførelse af ansvarlighedsprincippet, og glæder sig over en sådan tæt tilpasning.

¹¹ Se betragtning 13 i udkastet til afgørelse.

¹² Se betragtning 8-10 i udkastet til afgørelse.

¹³ Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

¹⁴ Behandlingsansvarlige i henhold til artikel 5, nr. IX, i LGPD.

- (9) Databeskyttelsesrådet bemærker, at LGPD med hensyn til konsekvensanalysen vedrørende databeskyttelse ikke indeholder en klar forpligtelse til at foretage konsekvensanalysen i tilfælde, hvor behandlingen kan medføre høj risiko for fysiske personers rettigheder og frihedsrettigheder, idet den kun henviser til en eventuel anmodning fra ANPD. I denne forbindelse bemærker Databeskyttelsesrådet, at ANPD anbefaler at foretage en konsekvensanalyse vedrørende databeskyttelse, når behandlingsaktiviteten kan medføre høj risiko, i de "ofte stillede spørgsmål"¹⁵ vedrørende konsekvensanalysen ("ofte stillede spørgsmål om konsekvensanalysen vedrørende databeskyttelse"). Desuden omfatter LGPD ikke udtrykkeligt vurderingen af nødvendigheden og proportionaliteten inden for rammerne af konsekvensanalysen vedrørende databeskyttelse. I de ofte stillede spørgsmål om konsekvensanalysen vedrørende databeskyttelse anbefales det imidlertid, at dataansvarlige og databehandlere vurderer nødvendigheden og proportionaliteten af behandlingen i deres konsekvensanalyser.
- (10) På denne baggrund opfordrer Databeskyttelsesrådet Kommissionen til at overvåge den praktiske gennemførelse af disse krav for at kontrollere, at konsekvensanalysen vedrørende databeskyttelse foretages, når behandlingen kan medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og at vurderingen af nødvendigheden og proportionaliteten af behandlingsaktiviteterne i forhold til formålene også indgår i konsekvensanalyserne vedrørende databeskyttelse.

2.2 Anvendelsesområde og definitioner

- (11) Kapitel 3 i referencen vedrørende et tilstrækkeligt beskyttelsesniveau omhandler indholdsprincipper og henviser til grundlæggende databeskyttelsesbegreber og -principper. Et system i et tredjeland eller en international organisation skal indeholde sådanne grundlæggende begreber og principper for at sikre et beskyttelsesniveau for personoplysninger, der i det væsentlige svarer til det, der er garanteret ved EU-retten. Terminologien skal ikke nødvendigvis være den samme som i databeskyttelsesforordningen, men begreberne bør afspejle og være i overensstemmelse med begreberne i EU's databeskyttelseslovgivning. Referencen vedrørende et tilstrækkeligt beskyttelsesniveau henviser til følgende vigtige begreber: "personoplysninger", "behandling", "dataansvarlig", "databehandler", "modtager" og "følsomme oplysninger". Dette aspekt af den brasilianske lov vil blive kommenteret i de næste afsnit.

2.2.1 LGPD's materielle og territoriale anvendelsesområde

- (12) Databeskyttelsesrådet glæder sig over, at LGPD's anvendelsesområde, både materielt og territorielt, er meget lig det, der er fastsat i EU's databeskyttelsesramme.
- (13) Artikel 4 i LGPD udelukker behandling til rent personlige og ikkeøkonomiske formål fra sit anvendelsesområde, og sådanne undtagelser findes også i databeskyttelsesforordningen (artikel 2, stk. 2, litra c), i databeskyttelsesforordningen). Desuden falder visse andre behandlingsaktiviteter delvis uden for LGPD's anvendelsesområde, navnlig behandling til følgende formål: offentlig sikkerhed, nationalt forsvar, nationale lovforanstaltninger eller efterforskning og retsforfølgning af straffbare handlinger, journalistiske og kunstneriske formål,

¹⁵ https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

akademisk arbejde/forskning og sundhedsforskning (artikel 3, nr. III, i LGPD). Dette er nærmere beskrevet i afsnit 3.1 i denne udtalelse.

- (14) Med hensyn til den delvise anvendelse af LGPD på behandling af personoplysninger, der foretages til journalistiske og kunstneriske formål, bemærker Databeskyttelsesrådet, at undtagelsens anvendelsesområde svarer til det, der er fastsat i artikel 85, stk. 2, i databeskyttelsesforordningen¹⁶, dvs. at en sådan undtagelse kun gælder, når personoplysninger udelukkende behandles til dette formål, og al anden behandling foretaget af presse, medier eller kunstneriske organer er omfattet af LGPD's anvendelsesområde. Visse undtagelser, der er fastsat for behandling af personoplysninger udelukkende til akademiske formål, dvs. artikel 7 (krav til retsgrundlag) og 11 (regler om behandling af følsomme oplysninger) i LGPD, finder fortsat anvendelse¹⁷. Anvendelsesområdet for disse undtagelser er også i overensstemmelse med det, der er fastsat i artikel 85, stk. 2, i databeskyttelsesforordningen.

2.2.2 Definitioner

- (15) Databeskyttelsesrådet noterer sig med tilfredshed tilpasningen til EU's databeskyttelsesramme i forbindelse med de definitioner, der anvendes i LGPD, og som er i overensstemmelse med definitionerne i databeskyttelsesforordningen. LGPD definerer navnlig "personoplysninger", "pseudonym information", "anonyme data"¹⁸, "databehandling", "dataansvarlig", "databehandler" og "følsomme oplysninger" (artikel 5 i LGPD) på lignende vis som i databeskyttelsesforordningen, nemlig betragtning 26, artikel 4 og artikel 9, stk. 1. Andre definitioner, f.eks. "registreret", "databeskyttelsesrådgiver", "samtykke", "konsekvensanalyse vedrørende databeskyttelse" og begrebet "fælles dataansvar"¹⁹ svarer også i det væsentlige til begreberne i databeskyttelsesforordningen.

2.3 Databeskyttelsesprincipper og retsgrundlag

2.3.1 Principper for behandlingen

- (16) Referencen vedrørende et tilstrækkeligt beskyttelsesniveau fastsætter i overensstemmelse med databeskyttelsesforordningen, at data skal behandles på en lovlig, retfærdig og legitim måde. I henhold til artikel 6 i LGPD skal aktiviteter i forbindelse med behandling af personoplysninger udføres i god tro og være underlagt følgende principper: formål, tilstrækkelighed, nødvendighed, fri adgang²⁰, datakvalitet, gennemsigtighed, sikkerhed, forebyggelse, ikkeforskelsbehandling, ansvar og ansvarlighed.
- (17) Under hensyntagen til begreberne i disse principper fastslår det brasilianske retssystem de samme databehandlingsprincipper, som er fastsat i artikel 5 i databeskyttelsesforordningen. For eksempel bestemmes det med hensyn til formålsbegrænsning i LGPD i artikel 7, stk. 7, at "[d]en efterfølgende behandling af personoplysninger, der er omhandlet i denne artikels stk. 3 (offentligt tilgængelige personoplysninger) og 4 (oplysninger, som tydeligvis er offentliggjort af

¹⁶ Se også betragtning 35 i udkastet til afgørelse.

¹⁷ Se også betragtning 32 og 33 i udkastet til afgørelse.

¹⁸ I artikel 12 i LGPD præciseres det yderligere, at anonymiserede data ikke betragtes som personoplysninger, medmindre anonymiseringen er eller kan blive omgjort ved en rimelig indsats. Det forklares, at "rimelig" skal vurderes under hensyntagen til objektive faktorer såsom: 1) omkostninger og tid, der er nødvendig for at omgøre anonymiseringen, 2) den tilgængelige teknologi, og 3) anvendelsen af kun den dataansvarliges egne midler.

¹⁹ Se artikel 42, stk. 1, nr. I, i LGPD.

²⁰ "Fri adgang: garanti til de registrerede om nem og gratis adgang til oplysninger om behandlingens form og varighed samt om integriteten af deres personoplysninger" (artikel 6, nr. IV, i LGPD).

den registrerede), kan foretages til nye formål, forudsat at legitime og specifikke formål med den nye behandling og bevarelsen af den registreredes rettigheder samt de grunde og principper, der er fastsat i denne lov, overholdes".

- (18) I databeskyttelsesforordningen kræves det klart, at en sådan efterfølgende behandling kun må finde sted, hvis et sådant nyt formål er foreneligt med det oprindelige formål. Kravet om at sikre formålenes forenelighed (samt overholdelse af gældende etiske standarder og tekniske og juridiske garantier) fremhæves i vejledningen om behandling af personoplysninger til akademiske formål og til gennemførelse af undersøgelser og forskning, som er udstedt af ANPD, samt i retningslinjerne om legitim interesse. ANPD forklarer i retningslinjerne om legitim interesse, hvordan den dataansvarlige skal påvise en effektiv forbindelse mellem de to formål med behandlingen og tage hensyn til den registreredes "legitime forventninger". I disse retningslinjer præciseres det endvidere, at "analysen af legitime forventninger kan baseres på flere faktorer, hvoraf følgende kan fremhæves: d) det tilsigtede formål med dataindsamlingen og dets forenelighed med behandling baseret på legitim interesse". Databeskyttelsesrådet glæder sig over en sådan præcisering fra ANPD, som bidrager til en bedre tilpasning af kravene til formålsbegrænsningen.
- (19) Ifølge princippet om opbevaringsbegrænsning i databeskyttelsesforordningen må oplysninger kun opbevares i det tidsrum, der er nødvendigt af hensyn til de formål, hvortil de behandles (artikel 5, stk. 1, litra e), i databeskyttelsesforordningen). Selv om artikel 6 i LGPD ikke udtrykkeligt indeholder princippet om opbevaringsbegrænsning, bør denne artikel læses sammen med artikel 15 i LGPD, der præciserer kravet i tilfælde af ophør af databehandlingen. I denne artikel er princippet om opbevaringsbegrænsning klart forbundet med principperne om "tilstrækkelighed" og "nødvendighed", som er blandt de generelle principper, der er anført i artikel 6 i LGPD. For at skabe større klarhed opfordrer Databeskyttelsesrådet Kommissionen til i udkastet til afgørelse at præcisere samspillet mellem artikel 6 og 15 i LGPD i forhold til princippet om opbevaringsbegrænsning.
- (20) Derudover fastsættes i artikel 16 i LGPD betingelserne for opbevaring og sletning af personoplysninger efter behandlingens ophør med hensyn til kravene om opbevaringsbegrænsning. Denne artikel fastsætter også fire formål, hvortil data kan opbevares efter afslutningen af databehandlingen: 1) for at opfylde juridiske eller forskriftsmæssige forpligtelser, 2) til forskningsformål, idet det så vidt muligt sikres, at oplysningerne anonymiseres, 3) når de overføres til tredjeparter i overensstemmelse med kravene i LGPD, eller 4) når de udelukkende anvendes af den dataansvarlige, så længe oplysningerne er anonymiserede, og tredjeparters adgang til disse oplysninger er forbudt. Databeskyttelsesrådet bemærker, at disse behandlingssituationer er i overensstemmelse med princippet om opbevaringsbegrænsning, der er nedfældet i databeskyttelsesforordningen.
- (21) Gennemsigtigheds- og rimelighedsprincippet har til formål at sikre, at de registrerede har kontrol over deres personoplysninger, og med dette formål for øje skal oplysninger som hovedregel proaktivt gives til den registrerede²¹. I mellemtiden fastsætter LGPD en begrænsning af dette princip når det drejer sig om "forretnings- og fabriks hemmeligheder", hvilket kan have betydning for de registreredes mulighed for at modtage oplysninger om behandlingen af deres oplysninger for at kunne udøve kontrol over den (f.eks. ved indgivelse af en klage til ANPD). Kommissionen forklarer imidlertid i udkastet til afgørelse, at denne begrænsning bør fortolkes i lyset af Brasiliens lov om adgang til oplysninger og præsidentielt dekret nr. 7.721 af 16. maj 2012 og derfor skal fortolkes således, at behandling og anden

²¹ Dette understreges også i referencen vedrørende et tilstrækkeligt beskyttelsesniveau, jf. kapitel 3, A(7).

videregivelse af oplysninger ikke må afsløre forretningshemmeligheder eller skabe konkurrencefordele for andre aktører, samtidig med at målene om beskyttelse af personoplysninger opfyldes. Med hensyn til gennemsigtighedsprincippet og i hele LGPD's tekst skal begrænsningen vedrørende "forretnings- og fabriks hemmeligheder" derfor ikke forstås som en generel begrundelse for ikke at overholde loven, men snarere at der skal indføres specifikke garantier for at sikre videregivelse af oplysninger på en måde, der beskytter disse interesser²².

- (22) I lyset af betydningen af gennemsigtighedsprincippet opfordrer Databeskyttelsesrådet Kommissionen til at overvåge gennemførelsen af denne bestemmelse i praksis for bedre at forstå dens indvirkning på retten til information og adgang.

2.3.2 Sikkerhedsforanstaltninger og -brud

- (23) LGPD omfatter sikkerheds- og forebyggelsesprincipper, der kræver, at der iværksættes foranstaltninger til beskyttelse af personoplysninger og forebyggelse af skader i forbindelse med en sådan behandling (artikel 6, nr. VII og VII, i LGPD). Desuden fastslår LGPD udtrykkeligt, at hvis sikkerhedsforanstaltninger ikke gennemføres korrekt, anses databehandling for at være ulovlig. Loven kræver, at der iværksættes de nødvendige foranstaltninger for at kunne påvise overholdelse af dette princip ved hjælp af en risikobaseret tilgang (artikel 44, 46 og 47 i LGPD), samt at kravene til vurdering og anmeldelse af brud følges (artikel 48 og 49 i LGPD). Databeskyttelsesrådet bemærker med tilfredshed, at sådanne principper og forpligtelser er nøje afstemt med dem, der er fastsat i databeskyttelsesforordningen.
- (24) Databeskyttelsesrådet glæder sig over, at ANPD har vedtaget en yderligere bindende forordning om underretning om sikkerhedshændelser, som fastlægger begrebet hændelse og nærmere bestemmelser om vurderingen af dens alvor (f.eks. hvornår hændelsen anses for at skabe risici for de registrerede eller i væsentlig grad påvirke de registreredes grundlæggende interesser og rettigheder og derfor skal meddeles til ANPD og de registrerede), samt kravene til underretning om hændelser²³. I denne forbindelse bemærker Databeskyttelsesrådet, at det ifølge forordningen om underretning om sikkerhedshændelser som hovedregel er den dataansvarlige, der skal meddele en sikkerhedshændelse til ANPD inden for tre arbejdsdage²⁴, og opfordrer Kommissionen til at tilpasse sit udkast til afgørelse (betragtning 75) i overensstemmelse hermed²⁵.
- (25) Med hensyn til underretning om brud på datasikkerheden bemærker Databeskyttelsesrådet, at LGPD fastslår, at en sådan underretning (til både ANPD og den registrerede) bl.a. skal indeholde oplysninger om tekniske og sikkerhedsmæssige foranstaltninger, der er anvendt til beskyttelse af personoplysninger, vedtaget før og efter hændelsen, under hensyntagen til forretnings- og fabriks hemmeligheder (artikel 6, nr. III, og artikel 9, nr. II, i LGPD). Databeskyttelsesrådet forstår nødvendigheden af effektivt at sikre, at retten til privatlivets fred og databeskyttelse ikke har negativ indvirkning på beskyttelsen af andre rettigheder, og opfordrer Kommissionen til at overvåge gennemførelsen af en sådan begrænsning, hvis der kun er givet delvise oplysninger om hændelsen (under hensyntagen til forretnings- og fabriks hemmeligheder), samt dens eventuelle indvirkning på ANPD's beføjelser.

²² Se betragtning 81 i udkastet til afgørelse.

²³ Se betragtning 73-77 i udkastet til afgørelse.

²⁴ Se artikel 6 og 9 i forordningen om underretning om sikkerhedshændelser.

²⁵ Se betragtning 75 i udkastet til afgørelse, ifølge hvilken anmeldelse af en sikkerhedshændelse til ANPD og de registrerede skal finde sted inden for tre dage (72 timer) efter, at den dataansvarlige er blevet opmærksom på den.

2.3.3 Lovlig behandling

- (26) Databeskyttelsesrådet bemærker, at lovlighedsprincippet og dets gennemførelse i LGPD (artikel 5, nr. XII, samt artikel 7, 8 og 10) ligger tæt op ad det, der er fastlagt i databeskyttelsesforordningen (artikel 4, nr. 11), samt artikel 6, 7 og 9), og hilser dette velkommen.

2.3.3.1 Legitim interesse

- (27) Kravene om legitim interesse, der kan anvendes som retsgrundlag for behandling i LGPD (artikel 7, nr. IX), er i overensstemmelse med databeskyttelsesforordningen (artikel 6, stk. 1, litra f)). I LGPD understreges det også, at de grundlæggende rettigheder og frihedsrettigheder (herunder retten til databeskyttelse²⁶) som udgangspunkt bør have forrang.
- (28) Databeskyttelsesrådet bemærker, at artikel 10 i LGPD opregner legitime formål, som et sådant retsgrundlag kan anvendes til. Et af disse legitime formål er at støtte og fremme den dataansvarliges aktivitet (artikel 10, nr. I, i LGPD).
- (29) Selv om dette udtryk synes at være bredt, bemærker Databeskyttelsesrådet, at betingelserne for anvendelsen af "legitim interesse" er nærmere beskrevet i vejledningen om retsgrundlag for behandling af personoplysninger vedrørende legitim interesse ("vejledningen om legitim interesse"), som er vedtaget af ANPD. Denne vejledning præciserer, at for at en interesse kan betragtes som "legitim", skal tre betingelser være opfyldt: 1) den skal være forenelig med det brasilianske retssystem, 2) den skal henvise til en specifik situation, og 3) behandlingen skal være knyttet til legitime, specifikke og udtrykkelige formål²⁷. Disse betingelser svarer til de tre kumulative betingelser for, at behandling af personoplysninger er lovlig i henhold til dette retsgrundlag, som er fastlagt af EU-Domstolen²⁸, samt Domstolens yderligere forklaringer. Desuden ligger betingelserne for den "legitime interesse", der er angivet i vejledningen om legitim interesse, tæt på dem i de retningslinjer, som Databeskyttelsesrådet har vedtaget²⁹. Databeskyttelsesrådet glæder sig over ANPD's tilgang til legitim interesse og dens anvendelse i forbindelse med behandling.

2.4 Individuelle rettigheder

- (30) Databeskyttelsesrådet glæder sig over, at LGPD giver enkeltpersoner lignende rettigheder som dem, der er fastsat i databeskyttelsesforordningen (begge i kapitel III). LGPD omfatter navnlig retten til indsigt, retten til berigtigelse, retten til dataportabilitet, retten til begrænsning af behandlingen, retten til sletning, retten til information, retten til at nægte eller tilbagetrække samtykke, retten til at gøre indsigelse mod behandlingen og retten til at indgive andragender (artikel 9 og 18 i LGPD).
- (31) LGPD giver også de registrerede ret til at anmode om en gennemgang af afgørelser, der udelukkende er truffet på grundlag af automatisk behandling af personoplysninger, og som påvirker deres interesser (artikel 20 i LGPD). Indholdet af artikel 20 i LGPD afspejler i det væsentlige artikel 22 i databeskyttelsesforordningen.

²⁶ Se punkt 3 i denne udtalelse.

²⁷ Se betragtning 52 i udkastet til afgørelse.

²⁸ F.eks. EU-Domstolen, 7. december 2023, dom i forenede sager C-26/22 og C-64/22, SCHUFA Holding AG, præmis 75-80.

²⁹ Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Version 1.0), vedtaget den 8. oktober 2024.

- (32) Databeskyttelsesrådet bemærker, at den brasilianske Habeas Data-lov i forbindelse med de registreredes rettigheder fastsætter specifikke bestemmelser for at give ret til indsigt og ret til berigtigelse inden for en kort frist (henholdsvis 10 og 15 dage) efter en persons anmodning, og glæder sig over dette.
- (33) Databeskyttelsesrådet er af den opfattelse, at LGPD i det væsentlige fastsætter tilsvarende krav til de registreredes rettigheder som dem, der er sikret i databeskyttelsesforordningen.

2.5 Begrænsninger for videreoverførsel

- (34) I referencen vedrørende et tilstrækkeligt beskyttelsesniveau præciseres det, at beskyttelsesniveauet for fysiske personer, hvis personoplysninger overføres i henhold til en tilstrækkelighedsafgørelse, ikke må undermineres af en videreoverførsel, og at enhver videreoverførsel derfor kun bør tillades, hvis den næste modtager (dvs. modtageren af videreoverførslen) også er underlagt regler (herunder kontraktlige regler), der sikrer et tilstrækkeligt beskyttelsesniveau og følger de relevante instrukser, når der behandles oplysninger på vegne af den dataansvarlige.
- (35) I forbindelse med tilstrækkelighedsvurderingen af Brasiliens retlige rammer og praksis betyder videreoverførsel overførsel af personoplysninger fra enheden, der fungerer som dataansvarlig, inden for LGPD's territoriale anvendelsesområde, til en enhed uden for dette anvendelsesområde.
- (36) Kravene til videreoverførsel er fastsat i kapitel V i LGPD og yderligere suppleret af ANPD gennem vedtagelsen af "dataoverførselsforordningen", som indeholder definitionerne af "overførsel", "international dataoverførsel", "importør" og "eksportør" og indeholder detaljerede krav til overførsler.
- (37) Databeskyttelsesrådet bemærker med tilfredshed, at definitionen af "overførsel" og "international dataoverførsel" er i overensstemmelse med dem i Databeskyttelsesrådets retningslinjer 05/2021³⁰.
- (38) I henhold til LGPD og dataoverførselsforordningen kan videreoverførsler kun finde sted til legitime, specifikke og udtrykkelige formål, og når der er indført specifikke instrumenter eller betingelser (artikel 33 i LGPD og artikel 9-33 i dataoverførselsforordningen)³¹. Databeskyttelsesrådet påskønner, at disse instrumenter ligger tæt på de overførselsværktøjer, der er fastsat i kapitel V i databeskyttelsesforordningen. Databeskyttelsesrådet opfordrer imidlertid Kommissionen til i udkastet til afgørelse at præcisere, om overførsler kun kan foretages i overensstemmelse med artikel 33, nr. III-IX, i LGPD under ekstraordinære omstændigheder, hvor betingelserne i artikel 33, nr. I-II, i LGPD ikke er opfyldt³².
- (39) Det præciseres imidlertid i dataoverførselsforordningen, at internationale overførsler af personoplysninger er tilladt, "når den registrerede har givet specifikt og særskilt samtykke til en sådan overførsel, efter at være blevet informeret om den påtænkte transaktions internationale karakter, og hvor dette klart adskilles fra andre formål". Det er ikke klart, om et

³⁰ Punkt 9, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, vedtaget den 14. februar 2023.

³¹ Se også betragtning 101-109 i udkastet til afgørelse.

³² I artikel 49 i databeskyttelsesforordningen fastsættes det, at de undtagelser, der er omhandlet i denne artikel, kun kan anvendes, hvis der ikke foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45, stk. 3, i databeskyttelsesforordningen, eller passende garantier i henhold til artikel 46 i databeskyttelsesforordningen.

sådan krav indebærer en forpligtelse til at informere de registrerede om de mulige risici ved internationale overførsler som følge af manglende tilstrækkelig beskyttelse i tredjelandet og manglende passende garantier (f.eks. oplysning om, at der måske ikke findes en tilsynsmyndighed og/eller databehandlingsprincipper og/eller registreredes rettigheder i tredjelandet), hvilket er et krav i henhold til artikel 49, stk. 1, litra a), i databeskyttelsesforordningen. For Databeskyttelsesrådet og i henhold til databeskyttelsesforordningen er det afgørende at give disse oplysninger for at gøre det muligt for den registrerede at give et informeret samtykke med fuldt kendskab til disse specifikke forhold ved overførslen. Databeskyttelsesrådet opfordrer derfor Kommissionen til i udkastet til afgørelse at præcisere, om den registrerede informeres om mulige risici ved en sådan overførsel som følge af manglende tilstrækkelig beskyttelse i tredjelandet og manglende fornødne garantier.

- (40) Desuden fastsættes det i dataoverførselsforordningen, at "både den dataansvarlige og databehandleren skal træffe effektive foranstaltninger, der kan påvise overholdelse af reglerne om beskyttelse af personoplysninger og effektiviteten af sådanne foranstaltninger på en måde, der er forenelig med risikoniveauet ved behandlingen og med den anvendte metode for international overførsel" (artikel 4, stk. 2, i dataoverførselsforordningen). Databeskyttelsesrådet glæder sig over medtagelsen af denne forpligtelse. Samtidig vil det være nyttigt at præcisere, at effektiviteten af disse foranstaltninger bør vurderes for også at sikre, at den lokale lovgivning i det relevante tredjeland ikke undergraver kontinuiteten i beskyttelsen af de registrerede, hvis data overføres³³. Databeskyttelsesrådet opfordrer Kommissionen til at præcisere, at dette element også vil blive taget i betragtning i overførselsscenarierne.
- (41) Databeskyttelsesrådet glæder sig over, at der er indført et udtrykkeligt gennemsigtighedskrav i forhold til den registrerede, dvs. at de registrerede har ret til at modtage det kontraktlige instrument, der anvendes til videreoverførslen, samt en beskrivelse af en sådan overførsel, f.eks. varighed og formål med overførslen, bestemmelseslandene, de involverede parter ansvar, de registreredes rettigheder og måder, hvorpå disse kan udøves (artikel 16 i dataoverførselsforordningen).
- (42) Det ser imidlertid ud til, at dette kun er relevant i forbindelse med gennemsigtighedsforpligtelsen, når overførsler foretages på grundlag af standardkontraktbestemmelser, og ikke når der anvendes andre værktøjer³⁴. Databeskyttelsesrådet opfordrer derfor Kommissionen til at præcisere, at de samme gennemsigtighedsforpligtelser gælder, uanset hvilket overførselsværktøj der anvendes.
- (43) Databeskyttelsesrådet bemærker også, at kravene til indholdet af de bindende virksomhedsregler ikke er fuldt ud i overensstemmelse med dem i databeskyttelsesforordningen, navnlig artikel 47, stk. 2, litra f) og l), i databeskyttelsesforordningen. For at sikre, at det beskyttelsesniveau, som databeskyttelsesforordningen giver, ikke undermineres, opfordrer Databeskyttelsesrådet Kommissionen til at præcisere i udkastet til afgørelse, at også disse elementer³⁵ vil blive taget

³³ Se Latombe-dommen. Se også EU-Domstolens dom af 16. juli 2020 i sag C-311/18 ("Schrems II").

³⁴ Dataoverførselsforordningen indeholder f.eks. generelle krav om gennemsigtighed, når det er hensigten at anvende de bindende virksomhedsregler, navnlig "etablering og gennemførelse af et program til forvaltning af privatlivets fred, som har til formål at skabe et tillidsforhold til den registrerede ved hjælp af gennemsigtige foranstaltninger, der sikrer mekanismer for den registreredes deltagelse" (artikel 25, nr. V, i dataoverførselsforordningen) og gennemsigtighed i forbindelse med udøvelsen af den registreredes rettigheder og ret til at klage (artikel 26, nr. VI, i dataoverførselsforordningen).

³⁵ Ansvar og samarbejde med tilsynsmyndigheden (artikel 47, stk. 2, litra f) og l), i databeskyttelsesforordningen).

i betragtning, når dette overførselsværktøj skal anvendes til videreoverførsel af personoplysninger, der overføres til Brasilien i henhold til tilstrækkelighedsafgørelsen.

2.6 Procedure- og håndhævelsesmekanismer

- (44) I henhold til referencen vedrørende et tilstrækkeligt beskyttelsesniveau³⁶ og til EU-Domstolens relevante praksis³⁷ skal et databeskyttelsessystem, der i det væsentlige svarer til EU-modellen, indeholde: i) en uafhængig myndighed, der skal føre tilsyn med og håndhæve databeskyttelseslovgivningen med beføjelse til at undersøge og træffe foranstaltninger uden påvirkning udefra. Databeskyttelsessystemerne skal sikre, at ii) dataansvarlige og databehandlere er ansvarlige og bevidste om deres ansvar, mens de registrerede informeres om deres rettigheder, og der bør være effektive sanktioner og kontrolprocedurer for at sikre overholdelse af reglerne iii) De dataansvarlige og databehandlere skal kunne påvise overholdelse gennem foranstaltninger såsom konsekvensanalyser vedrørende databeskyttelse, fortegnelser over behandlingsaktiviteter og udpegelse af databeskyttelsesansvarlige. Endvidere skal iv) databeskyttelsessystemet støtte og hjælpe de registrerede med at udøve deres rettigheder og omfatte passende søgsmålsmekanismer.
- (45) I dette afsnit har Databeskyttelsesrådet fokuseret sin vurdering på, hvorvidt der findes en uafhængig myndighed, en passende klagemekanisme og effektive sanktioner.

2.6.1 Uafhængigt tilsyn

- (46) I LGPD fastslås det, at Agencia Nacional de Proteção de Dados (ANPD) er den nationale tilsynsmyndighed med ansvar for at overvåge og håndhæve dens bestemmelser.
- (47) Databeskyttelsesrådet glæder sig over, at ANPD er blevet tildelt status som "myndighed af særlig karakter", som er en betegnelse, der skal sikre den autonomi, der er nødvendig for fuldt ud at udøve de juridiske funktioner og beføjelser, der er tillagt den ved LGPD, navnlig ved at ophæve bestemmelser, der krævede tilladelse fra den udøvende magt til ANPD's funktion og finansielle drift.
- (48) Databeskyttelsesrådet glæder sig ligeledes over de ændringer, der den 15. september 2025 blev foretaget i Brasiliens retlige ramme, i henhold til hvilken ANPD nu anerkendes som et **reguleringsorgan**³⁸. Databeskyttelsesrådet forstår derfor, at en af de vigtigste ændringer er, at ANPD vil forelægge sit budget direkte for ministeriet for planlægning og budget i stedet for at skulle forelægge det via justitsministeriet. ANPD's budget er fortsat en særskilt post på det føderale budget. Databeskyttelsesrådet forstår, at ANPD allerede var uafhængig også i forhold til sit budget og sin finansiering, men ved at blive et reguleringsorgan forenkles dets administrative proces.
- (49) Databeskyttelsesrådet glæder sig også over, at ANPD har fået nye beføjelser med udpegelsen som myndighed med ansvar for beskyttelsen af børn online³⁹. Databeskyttelsesrådet noterer sig, at ANPD i henhold til kapitel IX i LGPD har de nødvendige og tilgængelige beføjelser og

³⁶ Se kapitel 3(C) i referencen vedrørende et tilstrækkeligt beskyttelsesniveau.

³⁷ EU-Domstolen, 6. oktober 2015, dom i sag C-362/14, Schrems.

³⁸ Foreløbig foranstaltning nr. 1.317/2025, tilgængelig på <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

³⁹ Lov nr. 15.211/2025 om beskyttelse af børn og mindreårige i det digitale miljø, tilgængelig på: <https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619>.

opgaver til at sikre overholdelse af databeskyttelsesrettigheder og fremme bevidstheden, såsom undersøgelses- og sanktionsbeføjelser (artikel 55-J i LGPD).

- (50) Med hensyn til ANPD's personale og budget, som spiller en rolle for dets uafhængighed, noterer Databeskyttelsesrådet sig med tilfredshed den nylige beslutning om at øge personalet med mere end 200 nye stillinger⁴⁰.
- (51) Databeskyttelsesrådet bemærker, at ANPD ifølge artikel 55-C i LGPD nu består af en række organer⁴¹, herunder det nationale råd for beskyttelse af personoplysninger og privatlivets fred ("rådet"). Databeskyttelsesrådet noterer sig dets sammensætning, som også omfatter repræsentanter for den føderale udøvende magt, den lovgivende magt og den dømmende magt⁴². Databeskyttelsesrådet bemærker også, at Rådet ifølge artikel 58-B i LGPD bl.a. er ansvarligt for "i) at foreslå strategiske retningslinjer og tilvejebringe baggrundsoplysninger med henblik på udarbejdelsen af den nationale politik for beskyttelse af personoplysninger og privatlivets fred samt for ANPD's aktiviteter", og ii) "anbefale handlinger, der skal udføres af ANPD".
- (52) Navnlig med hensyn til disse opgaver finder Databeskyttelsesrådet det vigtigt at opnå en klarere forståelse af, hvordan de gennemføres, og i hvilket omfang Rådets forslag og henstillinger påvirker ANPD's arbejde. Det opfordrer derfor Kommissionen til at uddybe disse opgaver og samspillet mellem rådet og ANPD for bedre at kunne vurdere rådets indflydelse på ANPD's aktiviteter.

2.6.2 Klagemuligheder

- (53) Databeskyttelsesrådet glæder sig over den klagemekanisme, der er fastsat i LGPD, som også giver de registrerede ret til at indgive en klage til ANPD og til at anfægte dens afgørelse ved at indgive en appel til bestyrelsen. Enkeltpersoner kan derefter anke bestyrelsens afgørelser ved domstolene samt klage over ANPD for manglende overholdelse af sine forpligtelser i henhold til LGPD. Da forskellen mellem appellmuligheden og klagemuligheden ikke klart fremgår af udkastet til afgørelse, opfordrer Databeskyttelsesrådet Kommissionen til yderligere at præcisere, hvordan disse to muligheder fungerer, herunder om anvendelsen af klagemuligheden kun er begrænset til afvisning af at behandle en klage eller afvisning af en klages realitet.
- (54) Databeskyttelsesrådet glæder sig ligeledes over bestemmelsen om retten til kompensation for materielle og ikkematerielle skader samt kollektive retsmidler (artikel 22 i LGPD).

2.6.3 Sanktioner

- (55) Databeskyttelsesrådet minder om, at effektive og afskrækkende sanktioner kan spille en vigtig rolle for at sikre overholdelse af databeskyttelsesreglerne, da det er et tegn på den høje grad af ansvarlighed og bevidsthed, som systemet sikrer. Databeskyttelsesrådet glæder sig over de korrigerende beføjelser, som ANPD er blevet tildelt, som er blevet udøvet ved flere lejligheder⁴³, og som omfatter en række foranstaltninger såsom advarsel, bøder på op til to

⁴⁰ <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

⁴¹ I henhold til LGPD's artikel 55-C består ANPD af: bestyrelsen, som er det øverste ledelsesorgan, det nationale råd for beskyttelse af personoplysninger og privatlivets fred, disciplinærrådet, IV – ombudsmandens kontor, VI – kontoret for retlige anliggender, og VI – administrative enheder og specialiserede enheder, der er nødvendige for håndhævelsen af bestemmelserne i LGPD. Se også betragtning 126-130 i udkastet til afgørelse.

⁴² Se også betragtning 132 i udkastet til afgørelse og artikel 55-C i LGPD.

⁴³ Se ANPD's register over sanktioner: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/deciso-es-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

procent (2 %) af den involverede private juridiske enheds bruttoindtægter, dagbøder, blokering af personoplysninger i forbindelse med overtrædelsen, indtil den er bragt i orden, midlertidig suspension af de relevante databehandlingsaktiviteter og sletning af de pågældende personoplysninger (artikel 52 i LGPD)⁴⁴. Databeskyttelsesrådet opfordrer Kommissionen til at overvåge, om de anvendes på en ensartet måde, navnlig med hensyn til sanktioner.

- (56) Databeskyttelsesrådet noterer sig med tilfredshed, at ANPD har udstedt en (bindende) forordning om sanktioner. Denne forordning kategoriserer sanktioner i forskellige niveauer ved hjælp af objektive faktorer såsom typen og mængden af behandlede oplysninger eller indvirkningen på registreredes rettigheder og fastsætter en metode til beregning af bøder, hvilket er i overensstemmelse med kravene i artikel 83 i databeskyttelsesforordningen.

3. BRASILIANSKE OFFENTLIGE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT FRA DEN EUROPÆISKE UNION

- (57) I henhold til artikel 45, stk. 2, i databeskyttelsesforordningen er vurderingen af de begrænsninger og garantier, der er fastsat i brasiliansk ret med hensyn til brasilianske offentlige myndigheders adgang til og efterfølgende anvendelse af personoplysninger, der overføres til dataansvarlige og databehandlere i Brasilien med henblik på strafferetlig håndhævelse og nationale sikkerhedsformål ("myndighedsadgang"), et vigtigt element i testen for "væsentlig ækvivalens" som fortolket af EU-Domstolen.
- (58) Databeskyttelsesrådet noterer sig med tilfredshed den særlige opmærksomhed, som Kommissionen har rettet mod dette aspekt i udkastet til afgørelse, og de faktuelle oplysninger, den har fremlagt⁴⁵. Databeskyttelsesrådet undlader derfor at gengive de fleste af de faktuelle konklusioner og analyser i denne udtalelse. I stedet vurderer Databeskyttelsesrådet indgrebet fra det brasilianske system for myndighedsadgang med henblik på retshåndhævelse og national sikkerhed på grundlag af de fire elementer, som Databeskyttelsesrådet har fastlagt i de europæiske væsentlige garantier for overvågningsforanstaltninger, vedtaget den 10. november 2020⁴⁶:
- Garanti A – Klare, præcise og tilgængelige regler
 - Garanti B – Nødvendighed og proportionalitet hvad angår de legitime mål, der forfølges
 - Garanti C – Uafhængig tilsynsmekanisme
 - Garanti D – Effektive klagemuligheder for de enkelte personer.

⁴⁴ "Disse sanktioner kan pålægges offentlige eller private enheder. Dette gælder dog ikke bøder og dagbøder, som ikke kan pålægges offentlige enheder" (betragtning 135 i udkastet til afgørelse).

⁴⁵ Se betragtning 152-217 i udkastet til afgørelse.

⁴⁶ [Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger](#).

3.1 Brasilianske offentlige myndigheders adgang til og anvendelse af oplysninger med henblik på strafferetlig håndhævelse

3.1.1 Retlige rammer for strafferetlig håndhævelse

- (59) Databeskyttelsesrådet bemærker, at brasilianske retshåndhævende myndigheders adgang til og efterfølgende anvendelse af personoplysninger⁴⁷ reguleres af et system af retsakter af forskellig retlig karakter. Databeskyttelse og privatlivets fred, herunder brev- og kommunikationshemmelighed, er nedfældet i forfatningens artikel 5 som grundlæggende rettigheder. Databeskyttelsesrådet glæder sig navnlig over, at omfanget af beskyttelsen af sådanne rettigheder, ligesom i EU, ikke er begrænset til brasilianske statsborgere, men også omfatter udlændinge, uanset om de er bosiddende i Brasilien eller ej⁴⁸.
- (60) Dernæst er der flere specialiserede sektorspecifikke love, der regulerer den mulige adgang til personoplysninger med henblik på retshåndhævelse. Hvad angår en sådan adgang til oplysninger, der overføres til Brasilien fra EU, er straffeloven, lov om telefonaflytning, den civile ramme for internettet, lov om finansielle institutioners fortrolighed, lov om kriminelle organisationer og strafferetlig efterforskning samt andre love særlig relevante. Databeskyttelsesrådet bemærker, at disse retsakter er offentligt tilgængelige og kan anses for at være tilstrækkeligt klare til at give de registrerede en indikation af de omstændigheder og betingelser, hvorunder offentlige myndigheder har beføjelse til at få adgang til deres data⁴⁹.
- (61) En anden vigtig retskilde i Brasilien er praksis fra Brasiliens føderale højesteret, som synes at anvende en bred fortolkning af anvendelsesområdet for rettighederne til privatlivets fred og databeskyttelse⁵⁰, samt praksis fra Den Interamerikanske Menneskerettighedsdomstol, der er ansvarlig for fortolkning og anvendelse af den amerikanske menneskerettighedskonvention, som Brasilien ratificerede i 1992⁵¹.
- (62) Databeskyttelsesrådet bemærker, at LGPD kun delvist finder anvendelse på tilfælde af behandling af personoplysninger med henblik på strafferetlig håndhævelse, hvilket kan føre til retsusikkerhed.
- (63) Som anerkendt af Kommissionen i udkastet til afgørelse finder LGPD ikke anvendelse på databehandling, der foretages *udelukkende* med henblik på offentlig sikkerhed, nationalt forsvar, statens sikkerhed eller efterforskning og retsforfølgning af straffbare handlinger⁵². I henhold til artikel 4, nr. I og III, i LGPD vil databehandling på disse områder være underlagt specifik lovgivning, som skal omfatte principperne og de registreredes rettigheder, der er skitseret i LGPD. Så vidt Databeskyttelsesrådet ved, og som Kommissionen har bekræftet, har Brasilien endnu ikke vedtaget specifik lovgivning om behandling af personoplysninger på

⁴⁷ Se listen over myndigheder i betragtning 165 i udkastet til afgørelse.

⁴⁸ Se betragtning 8 og 9 i udkastet til afgørelse.

⁴⁹ Se Menneskerettighedsdomstolens dom i Zakharov-sagen, præmis 229.

⁵⁰ Se Brasiliens føderale højesteret, afgørelse om ADI 6649, september 2022.

⁵¹ Se betragtning 10 i udkastet til afgørelse.

⁵² Se betragtning 30 og 31 i udkastet til afgørelse.

strafferets- og retshåndhævelsesområdet (f.eks. svarende til EU's retshåndhævelsesdirektiv⁵³).

- (64) Databeskyttelsesrådet noterer sig med tilfredshed, at Brasiliens føderale højesteret i sin praksis⁵⁴ har fortolket LGPD på en måde, der udvidede dens delvise anvendelse til behandling af personoplysninger med henblik på strafferetlig efterforskning og opretholdelse af den offentlige orden.
- (65) Databeskyttelsesrådet glæder sig over, at Brasiliens tilsynsmyndighed, ANPD, fuldt ud støtter denne fortolkning og mener, at "fraværet af specifik lovgivning ikke giver sikkerhedsmyndigheder en bred og ubegrænset tilladelse til at behandle borgernes personoplysninger udelukkende med henblik på offentlig sikkerhed samt efterforskning og retsforfølgning af strafbare handlinger uden nogen begrænsninger"⁵⁵. Samtidig bemærker Databeskyttelsesrådet, at ANPD i henhold til LGPD's artikel 4, nr. III, stk. 3, for visse specifikke behandlinger af oplysninger, der udelukkende foretages med henblik på retshåndhævelse, i øjeblikket hovedsagelig synes at have en rådgivende rolle over for de retshåndhævende myndigheder.
- (66) Databeskyttelsesrådet opfordrer Kommissionen til i udkastet til afgørelse yderligere at vurdere og præcisere anvendelsen af LGPD i tilfælde af behandling af personoplysninger med henblik på strafferetlig håndhævelse, herunder ANPD's beføjelser, samt til nøje at tage hensyn til enhver relevant udvikling i denne henseende i sin fremtidige overvågning (se også afsnittet om tilsyn og klagemuligheder).

3.1.2 Nødvendighed og proportionalitet

- (67) Databeskyttelsesrådet bemærker med tilfredshed, at det som hovedregel kræver forudgående retskendelse at få adgang til kommunikationsdata, både indhold og metadata, samt til andre kategorier af beskyttede fortrolige oplysninger såsom bank- og skattedata.
- (68) For så vidt angår adgang til kommunikationsdata glæder Databeskyttelsesrådet sig over, at en sådan foranstaltning i henhold til loven om telefonaflytning og den føderale højesterets praksis betragtes som en undtagelse og er underlagt strenge betingelser, der har til formål at sikre dens nødvendighed og proportionalitet⁵⁶. Som en forebyggende foranstaltning mod muligt misbrug fastsætter brasiliansk ret desuden, at aflytning af kommunikation uden en retskendelse eller til formål, der ikke er tilladt i henhold til loven, udgør en forbrydelse, der kan straffes med op til fire års fængsel⁵⁷.
- (69) En streng gennemførelse af garantierne for adgang til kommunikationsdata er særlig relevant, da der i Brasilien findes en generel forpligtelse for udbydere af internetforbindelser og onlineapplikationstjenester til at opbevare forbindelseslogfiler i et år⁵⁸. Databeskyttelsesrådet noterer sig med tilfredshed, at adgang til de lagrede data kun er mulig, hvis der foreligger en retskendelse⁵⁹. Det minder om den strenge tilgang og de begrænsninger, der gælder for

⁵³ Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89).

⁵⁴ Se Brasiliens føderale højesteret, afgørelse om ADI 6649, september 2022.

⁵⁵ Se ANPD's tekniske notat nr. 29/2024/FIS/CGF/ANPD, adresseret til justitsministeriet og ministeriet for offentlig sikkerhed, punkt 5.4.1.29, som kan findes på: [SEI/ANPD – 0132350 – Nota Técnica](#).

⁵⁶ Se betragtning 169 og 170 i udkastet til afgørelse.

⁵⁷ Ibid.

⁵⁸ Se betragtning 173 i udkastet til afgørelse.

⁵⁹ Ibid.

generel og udifferentieret lagring af kommunikationsmetadata i EU⁶⁰, og noterer sig med tilfredshed de yderligere oplysninger fra Kommissionen om fraværet af masselagring af data i landet. Databeskyttelsesrådet opfordrer derfor Kommissionen til at være særlig opmærksom på den retlige ordning og praksis i Brasilien vedrørende adgang til kommunikationsdata under overvågningen og revisionen af udkastet til afgørelse.

- (70) Databeskyttelsesrådet bemærker med tilfredshed, at lignende garantier også gælder for retshåndhævende myndigheders adgang til skatte- og bankoplysninger, dvs. krav om forudgående retskendelse, kun tilladt ved alvorlige forbrydelser, eksistensen af strafferetlige sanktioner i tilfælde af misbrug osv.
- (71) Ifølge udkastet til afgørelse er der en undtagelse fra det generelle krav om forudgående retskendelse for retshåndhævende myndigheders adgang til visse kategorier af personoplysninger⁶¹. I henhold til artikel 15 og 16 i lov om kriminelle organisationer og strafferetlig efterforskning kan en politichef og anklagemyndigheden uden retskendelse få adgang til en efterforsket persons registreringsoplysninger om vedkommende: "personlige kvalifikationer, tilhørsforhold og adresse, som opbevares af valgdomstolen, telefonselskaber, finansielle institutioner, internetudbydere og kreditkortadministratorer"⁶². På samme måde vil transportvirksomhederne i en periode på fem år give en dommer, anklagemyndigheden eller en politichef direkte og permanent adgang til databaserne over reservationer og rejseoplysninger⁶³.
- (72) Databeskyttelsesrådet bemærker, at anvendelsesområdet for lov om kriminelle organisationer og strafferetlig efterforskning er begrænset til efterforskning og sanktionering af organiserede kriminelle grupper og terrororganisationer, som udgør en betydelig risiko for borgerne og samfundet, hvilket derfor kan begrunde et mere alvorligt indgreb i de grundlæggende rettigheder til privatlivets fred og databeskyttelse⁶⁴. Samtidig mener Databeskyttelsesrådet, at oplysningerne om disse undtagelser i betragtning 164 i udkastet til afgørelse er meget generelle og ikke fuldstændige. Det fremgår navnlig ikke klart af oplysningerne i udkastet til afgørelse, om adgangen til personoplysninger i så fald er underlagt efterfølgende domstolsprøvelse af nødvendigheden og proportionaliteten.
- (73) I lyset heraf opfordrer Databeskyttelsesrådet Kommissionen til i udkastet til afgørelse yderligere at præcisere og forklare omfanget og arten af de tilfælde, hvor retshåndhævende myndigheders adgang til data ikke kræver retskendelse, samt de gældende garantier i den brasilianske lovgivning. Databeskyttelsesrådet mener også, at Kommissionen bør være særlig opmærksom på anvendelsen af disse undtagelser i henhold til brasiliansk ret under sin overvågning af udkastet til afgørelse.

3.1.3 Videre anvendelse af data og videreoverførsler

- (74) Databeskyttelsesrådet minder om, at beskyttelsesniveauet for personoplysninger, der overføres fra EU/EØS til Brasilien, ikke må undermineres af yderligere brug eller deling af oplysningerne med modtagere i Brasilien eller i et tredjeland, dvs. at videreoverførsler kun bør

⁶⁰ Der findes yderligere oplysninger om datalagring i Databeskyttelsesrådets erklæring 5/2024 om henstillingerne fra Gruppen på Højt Plan om Adgang til Data med henblik på Effektiv Retshåndhævelse, der findes på https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehigh_en.pdf.

⁶¹ Se betragtning 164 i udkastet til afgørelse.

⁶² Se artikel 15 i lov om kriminelle organisationer og strafferetlig efterforskning.

⁶³ Se artikel 16 i lov om kriminelle organisationer og strafferetlig efterforskning.

⁶⁴ Se Domstolens dom af 6. oktober 2020, forenede sager La Quadrature du Net m.fl., C-511/18 og C-512/18, EU:C:2020:791, præmis 95-98, dom af 2. oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 54, 57 og 60, dom af 2. marts 2021, Prokuratuur (Betingelser for adgang til data vedrørende elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 35.

tillades, hvis der sikres et fortsat beskyttelsesniveau, der i det væsentlige svarer til det, der er fastsat i EU-retten.

- (75) I denne forbindelse noterer Databeskyttelsesrådet sig med tilfredshed, at Brasiliens føderale højesteret har fastslået, at deling af personoplysninger mellem offentlige organer (herunder når de deles mellem retshåndhævende myndigheder og efterretningstjenester) forudsætter: 1) definition af et legitimt, specifikt og udtrykkeligt formål med databehandlingen, 2) behandlingens forenelighed med de oplyste formål, 3) begrænsning af delingen til det minimum, der er nødvendigt for at opfylde det oplyste formål, samt fuld overholdelse af de krav, garantier og procedurer, der er fastsat i LGPD, for så vidt som det er foreneligt med den offentlige sektor"⁶⁵.
- (76) Uanset denne vigtige afgørelse fra den højeste domstol i Brasilien, og i betragtning af den allerede nævnte kompleksitet samt det præcise omfang af og de nærmere bestemmelser om anvendelsen af LGPD på retshåndhævende myndigheder, opfordrer Databeskyttelsesrådet Kommissionen til nøje at overvåge udviklingen og praksis på dette område.
- (77) Med hensyn til videreoverførsel af personoplysninger til strafferetlige retshåndhævende myndigheder i tredjelande henvises der i udkastet til afgørelse til artikel 33, nr. III, i LGPD, som fastsætter, at internationale dataoverførsler kan finde sted, når det er "nødvendigt for internationalt retligt samarbejde mellem offentlige organer for efterretning, efterforskning og retsforfølgning i overensstemmelse med internationale retlige instrumenter" ⁶⁶ . Databeskyttelsesrådet anser denne forklaring for at være for generel og opfordrer Kommissionen til i udkastet til afgørelse at uddybe betingelserne og garantierne for videreoverførsler yderligere.

3.1.4 Tilsyn og klagemuligheder

- (78) Databeskyttelsesrådet minder om, at ethvert indgreb i retten til privatlivets fred og databeskyttelse bør være underlagt et effektivt, uafhængigt og upartisk tilsynssystem, som enten en dommer eller et andet uafhængigt organ (f.eks. en administrativ myndighed eller et parlamentarisk organ) stiller til rådighed⁶⁷.
- (79) Det bemærkes også, at inden for de brasilianske rammer, som beskrevet af Kommissionen, overvåges de strafferetlige håndhævende myndigheders aktiviteter af forskellige organer: i) den dømmende magt, ii) ANPD og iii) anklagemyndigheden.
- (80) Domstolskontrollen, som forklaret ovenfor i afsnittet om nødvendighed og proportionalitet⁶⁸, finder anvendelse i forbindelse med indsamling af og adgang til personoplysninger, navnlig i form af forudgående gennemgang og godkendelse.
- (81) Med hensyn til ANPD's rolle mindes der i udkastet til afgørelse om tilstrækkeligheden, som allerede forklaret i afsnit 3.1.1. i denne udtalelse, om, at denne lov i henhold til artikel 4, nr. III, i LGPD ikke finder anvendelse på behandling af personoplysninger, der foretages *udelukkende* med henblik på i) den offentlige sikkerhed, ii) det nationale forsvar, iii) statens sikkerhed og iv) efterforskning og retsforfølgning af strafbare handlinger. Desuden fremgår

⁶⁵ Se betragtning 187 i udkastet til afgørelse.

⁶⁶ Ibid.

⁶⁷ Anbefalinger 02/2020 om de europæiske væsentlige garantier for overvågningsforanstaltninger, vedtaget den 10. november 2020, se side 12, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

⁶⁸ Se afsnit 3.1.2 ovenfor.

det af artikel 4, nr. I, at en sådan behandling vil være omfattet af specifik lovgivning, som bl.a. skal omfatte de generelle principper for beskyttelse og de registreredes rettigheder, som beskrevet i LGPD. I samme artikels stk. 3 anerkendes ANPD's rådgivende rolle i forbindelse med de undtagelser, der er fastsat i nr. III, når de udelukkende gennemføres med disse formål for øje, navnlig ANPD's beføjelser til at afgive tekniske udtalelser og henstillinger samt til at anmode de relevante dataansvarlige om konsekvensanalyser vedrørende databeskyttelse.

- (82) I sit udkast til afgørelse⁶⁹ henviser Kommissionen til en vigtig afgørelse af 15. september 2022 fra den føderale højesteret, som angiver, at generelle databeskyttelsesprincipper og registreredes rettigheder finder anvendelse på statens behandling af personoplysninger med henblik på levering af offentlige tjenester. Denne afgørelse fokuserer på "deling af personoplysninger" mellem organer og enheder i den offentlige forvaltning og i efterretningsaktiviteter samt på "offentlige organers og enheders adgang" til registret over borgernes data. Med hensyn til ANPD's håndhævelsesrolle forstår Databeskyttelsesrådet ud fra yderligere oplysninger fra Kommissionen, at ANPD allerede har udøvet en sådan rolle over for politiet samt over for justitsministeriet og ministeriet for offentlig sikkerhed. Dette blev gjort på grundlag af retspraksis, som ved at udvide den delvise anvendelse af generelle principper og registreredes rettigheder til også at omfatte behandling med henblik på retshåndhævelse gør ANPD ansvarlig for også at føre tilsyn med og håndhæve lovgivningen på dette område.
- (83) I lyset af ovenstående opfordrer Databeskyttelsesrådet Kommissionen til yderligere at uddybe ANPD's håndhævelsesrolle, navnlig med hensyn til de relevante retsgrundlag samt dens undersøgelsesbeføjelser og korrigerende beføjelser over for retshåndhævende myndigheder, og til nøje at overvåge udviklingen på dette område.
- (84) Endelig bemærker Databeskyttelsesrådet, at anklagemyndigheden har en bredere kompetence end blot at føre tilsyn med reglerne om databeskyttelse og privatlivets fred og pålægge sanktioner for krænkelse af grundlæggende rettigheder. Som allerede forklaret i afsnit 3.1 i denne udtalelse, er anklagemyndigheden i henhold til lov om kriminelle organisationer og strafferetlig efterforskning f.eks. en af de myndigheder, der uden retskendelse kan få adgang til registreringsoplysninger om en efterforsket person. Databeskyttelsesrådet opfordrer derfor Kommissionen til i udkastet til afgørelse yderligere at uddybe og forklare anklagemyndighedens rolle og beføjelser i forbindelse med tilsynet med de brasilianske retshåndhævende myndigheders behandling af personoplysninger.
- (85) Med hensyn til klageadgang bemærker Databeskyttelsesrådet med tilfredshed, at de retlige mekanismer, der er beskrevet i første del af denne udtalelse, og navnlig de retsmidler, der er til rådighed for enkeltpersoner til at håndhæve deres ret til databeskyttelse og privatlivets fred, også finder anvendelse i forbindelse med de strafferetlige håndhævelsesmyndigheders aktiviteter.

3.2 De brasilianske offentlige myndigheders adgang til og brug af personoplysninger til nationale sikkerhedsformål

⁶⁹ Se betragtning 187 i udkastet til afgørelse.

3.2.1 Anvendelsesområdet for undtagelsen i artikel 4, nr. III, i LGPD og dens anvendelse på strafbare handlinger mod statens sikkerhed

- (86) Som Kommissionen har forklaret, undtager artikel 4, nr. III, i LGPD "statens sikkerhed" fra anvendelsen af LGPD ved behandling af personoplysninger, sammen med offentlig sikkerhed, nationalt forsvar samt aktiviteter i forbindelse med efterforskning og retsforfølgning af strafbare handlinger.
- (87) Databeskyttelsesrådet bemærker, at den brasilianske lovgivning om "Seguranca Nacional" (national sikkerhed), som fastsat i lov nr. 14.197 af 1. september 2021, der ændrer straffeloven og ophæver loven af 1983 om national sikkerhed⁷⁰, udtrykker det brasilianske begreb om national sikkerhed på grundlag af en udtømmende liste over strafbare handlinger⁷¹, som omhandler forskellige trusler mod den brasilianske stats integritet som institution (national suverænitet, spionage (art. 350-K), forbrydelser mod de demokratiske institutioner (art. 359-L) m.fl.). Bestemmelserne i lov nr. 14.197 er blevet gjort til en integreret del af den brasilianske straffelov.
- (88) Når det er sagt, forventer Databeskyttelsesrådet, at de brasilianske myndigheders behandling af oplysninger med henblik på retsforfølgning af de lovovertrædelser, der er fastsat i lov nr. 14.197, er omfattet af den ordning, der gælder for brasilianske myndigheders adgang til og brug af oplysninger med henblik på strafferetlig håndhævelse, som beskrevet i kapitel 3.2 i udkastet til afgørelse, og dermed er underlagt de samme overvejelser om databeskyttelse som anført i kapitel 3.1 i denne udtalelse. Databeskyttelsesrådet anmoder derfor Kommissionen om at præcisere i udkastet til afgørelse, om databehandlingen i forbindelse med retsforfølgning af de strafbare handlinger, der er opført i lov nr. 14.197, faktisk er omfattet af den databeskyttelsesordning, der gælder for retshåndhævelsesaktiviteter, eller af en anden ordning. Hvis sidstnævnte er tilfældet, opfordrer Databeskyttelsesrådet Kommissionen til at redegøre nærmere for de databeskyttelsesregler, der gælder for strafferetlig forfølgning af disse lovovertrædelser af hensyn til den nationale sikkerhed.

3.2.2 Retsgrundlag for national sikkerhed

- (89) Den kodificerede retlige ramme, som udkastet til afgørelse baserer sine konklusioner på i kapitlet om myndighedsadgang til "nationale sikkerhedsformål", består af lov nr. 14.197 fra 2021, lov nr. 9.883 af 7. december 1999 om oprettelse af det brasilianske efterretningssystem og det tilhørende dekret nr. 4.376 af 2002. De to sidstnævnte retsakter etablerer det brasilianske efterretningssystem (Sistema Brasileiro de Inteligência (SISBIN)) og dets funktion. De efterfølges af det bindende præsidentdekret nr. 8.793⁷² af 2016, der definerer den nationale efterretningspolitik (den såkaldte "Política Nacional de Inteligência" (PNI)), samt LGPD fra 2018.
- (90) Præsidentielt dekret nr. 8.793 af 2016 beskriver emnet, målene og grænserne for PNI. Aktiviteter i henhold til dette dekret har til formål at frembringe og udbrede viden til de kompetente myndigheder om forhold og situationer, der opstår inden for eller uden for det nationale område, med umiddelbar eller potentiel indflydelse på beslutningsprocessen,

⁷⁰ Lov nr. 14.197 af 1. september 2021, som findes på https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/14197.htm (02.10.2026).

⁷¹ Se betragtning 200 i udkastet til afgørelse.

⁷² Se betragtning 199 i udkastet til afgørelse.

statslige tiltag samt samfundets og statens sikkerhed og efterretninger. Under disse omstændigheder henviser efterretning til alle de oplysninger – og data, der kræves og behandles for at understøtte den udøvende magts beslutningsproces på dette område.

- (91) I henhold til retsgrundlaget for SISBIN, som fremlagt af Kommissionen, er SISBIN og dets enheder blevet oprettet som den centrale mekanisme til gennemførelse af PNI og har som sådan til opgave at udføre aktiviteter vedrørende national sikkerhed samt offentlig sikkerhed og beskyttelse af demokratiske institutioner. Med henblik herpå giver SISBIN mulighed for vidensudveksling og integreret planlægning af aktiviteter⁷³. Som følge heraf er begrebet national sikkerhed i Brasilien i lyset af SISBIN's aktiviteter tilsyneladende ikke begrænset til de strafbare handlinger, der er kodificeret i lov nr. 14.197, men kan betragtes som en integreret del af et bredere begreb om national efterretning.
- (92) Da SISBIN blev oprettet, bestod den af 18 føderale enheder, herunder 13 ministerier, og blev efterfølgende udvidet til 48 såkaldte agenturer i henhold til dekret nr. 11.693 af 6. september 2023 om SISBIN's organisation og funktion⁷⁴. Databeskyttelsesrådet bemærker, at samarbejdet inden for SISBIN omfatter enheder ud over de klassiske sikkerhedsinstitutioner, såsom videnskabsministeriet (artikel 4, nr. IV), landbrugsministeriet (artikel 4, nr. XV) og energiministeriet (artikel 4, nr. XVIII) samt forbundsanklageren (artikel 4, nr. XIX).
- (93) Hvor dekret nr. 4.376 af 2002 har pålagt det rådgivende råd for det brasilianske efterretningssystem at foreslå generelle standarder og procedurer for udveksling af "viden og kommunikation" inden for SISBIN⁷⁵, pålægger dekret nr. 11.693 af 2023 SISBIN's centrale organ at udvikle tekniske værktøjer⁷⁶ til deling af information, data og viden og beskriver delingen og anvendelsen af data, der er indhentet af SISBIN's enheder. Kommissionens udkast til afgørelse indeholder imidlertid ingen yderligere oplysninger om sådanne regler eller retlige standarder udstedt af det centrale organ, f.eks. når SISBIN's enheder deler personoplysninger indbyrdes.
- (94) Desuden synes der at være forskelle i begreberne om oplysningers følsomhed, idet følsomhed ifølge den relevante lovgivning, der regulerer SISBIN's aktiviteter, er knyttet til den grad af fortrolighed, der gives en oplysning⁷⁷, og til formålsbegrænsning sammenlignet med de generelle principper i databeskyttelsesforordningen⁷⁸.
- (95) Som allerede forklaret ovenfor, undtager artikel 4, nr. III, litra a)-c), i LGPD, som først blev kodificeret efter oprettelsen af SISBIN og fastlæggelsen af en national efterretningspolitik, databehandlingsaktiviteter, der udelukkende udføres af hensyn til den offentlige sikkerhed, det nationale forsvar og statens sikkerhed, fra anvendelsen af LGPD, bortset fra de fastsatte generelle databeskyttelsesprincipper.
- (96) Som understreget af Kommissionen i udkastet til afgørelse, vedrører den overordnede ramme i den brasilianske forfatning samt Brasiliens deltagelse i Den Interamerikanske Menneskerettighedsdomstol den retlige ramme for myndighedsadgang med henblik på nationale efterretningstjenester. Databeskyttelsesrådet anerkender også, at afgørelserne fra

⁷³ I præsidentielt dekret nr. 8.793, afsnit 5, nævnes SISBIN og de organer, der er integreret deri, vidensudveksling inden for SISBIN og integreret planlægning af samarbejdet mellem medlemmerne af SISBIN som instrumenter til gennemførelse af PNI.

⁷⁴ Se betragtning 202 i udkastet til afgørelse.

⁷⁵ Se artikel 7, nr. II, i dekret nr. 4.376.

⁷⁶ Se artikel 10, nr. XI, som findes på https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm (26.9.2025).

⁷⁷ Se dekret nr. 8.793 af 2016, dekret nr. 11.693, betragtning 204 i udkastet til afgørelse.

⁷⁸ Se artikel 6, nr. I, i LGPD, som vedrører legitime og specifikke formål, mens databeskyttelsesforordningen kræver lovlige og specifikke formål.

Brasiliens føderale højesteret har spillet en vigtig rolle med hensyn til at definere reglerne⁷⁹. Højesterets afgørelser har indtil videre været en præcis og relevant støtte til den videre udvikling af beskyttelsen af personoplysninger i overensstemmelse med den brasilianske forfatning. Samtidig skal det bemærkes, at højesterets afgørelser ikke præciserer eller fastsætter generelle abstrakte databeskyttelsesregler for behandling af personoplysninger, men fortolker bestemmelserne og principperne i forfatningen og LGPD.

- (97) Databeskyttelsesrådet er opmærksom på, at staterne har en bred skønsmargen til at definere spørgsmål om national sikkerhed, hvilket derefter muliggør undtagelser af hensyn til den nationale sikkerhed i forbindelse med behandling af personoplysninger. I denne sammenhæng minder det om Den Europæiske Menneskerettighedsdomstols definition, ifølge hvilken trusler mod den nationale sikkerhed skal kunne skelnes fra generelle risici for den offentlige sikkerhed eller fra alvorlige strafbare handlinger på grund af deres art, alvor og særlige omstændigheder⁸⁰.
- (98) Det er Databeskyttelsesrådets opfattelse, at oplysninger, der behandles af SISBIN's enheder, kun er omfattet af undtagelsen i artikel 4, nr. III, i LGPD, når behandlingen *udelukkende* foretages af hensyn til den offentlige sikkerhed, det nationale forsvar og statens sikkerhed. Dette synes at gælde specifikt for aktiviteterne i SISBIN's centrale organ, den brasilianske efterretningstjeneste (ABIN). Derfor finder LGPD fuld anvendelse, medmindre en enhed i SISBIN handler på vegne af ABIN til et af disse formål.
- (99) Databeskyttelsesrådet opfordrer Kommissionen til at bekræfte denne forståelse og til i udkastet til afgørelse mere præcist at beskrive og forklare rammerne for begrebet national sikkerhed i henhold til brasiliansk ret, navnlig i relation til indsamling og deling af data mellem og af enheder i forbindelse med SISBIN's aktiviteter samt med hensyn til gennemførelsen af PNI. I denne forbindelse opfordrer Databeskyttelsesrådet Kommissionen til også at præcisere, hvordan undtagelser fra LGPD af hensyn til den nationale sikkerhed forholder sig til undtagelsen for den nationale sikkerhed i henhold til databeskyttelsesforordningen.

3.2.3 Videreoverførsler og internationale aftaler

- (100) I artikel 33 i LGPD defineres forudsætningerne for international dataoverførsel. I artikel 33, nr. I og II, i LGPD fastsættes krav svarende til en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller kravene om yderligere garantier i henhold til databeskyttelsesforordningen. Disse krav fraviges i artikel 33, nr. III, VI og VII, i LGPD, som omhandler tilfælde af "retligt samarbejde mellem efterretningstjenester", overførsler, der sker som følge af "en forpligtelse indgået i internationale samarbejdsaftaler", og overførsler, der "kræves for håndhævelse af en offentlig politik eller at give offentlige tjenester status som juridisk person", dvs. national sikkerhed og efterretning. Denne afgørelse synes at være i overensstemmelse med begrebet i artikel 4, nr. III, i LGPD, som begrænser anvendelsen af LGPD til udelukkende at omfatte dens principper med hensyn til spørgsmål om offentlig sikkerhed, nationalt forsvar og statens sikkerhed. Det kan således antages, at videreoverførsler til nationale efterretningsformål bør ske i overensstemmelse med de generelle principper for databeskyttelse i LGPD og samtidig være underlagt bestemmelserne om internationalt samarbejde i retsakterne om oprettelse af PNI og SISBIN.
- (101) Når det er sagt, anerkender Databeskyttelsesrådet, at Brasilien kan have behov for at videregive og faktisk videregiver personoplysninger til udenlandske efterretningstjenester med

⁷⁹ Se betragtning 203 i udkastet til afgørelse.

⁸⁰ Den Europæiske Menneskerettighedsdomstol, Big Brother Watch m.fl. mod Det Forenede Kongerige, 25. maj 2021, § 350.

henblik på samarbejde eller med henblik på at gennemføre PNI i overensstemmelse med målet om at forebygge og identificere trusler på grundlag af det ovennævnte integrerede sikkerhedsbegreb.

- (102) Som tidligere nævnt påpeger Kommissionen, at den overordnede ramme i den brasilianske forfatning og garantien i Habeas Data gælder for beskyttelse af personoplysninger inden for SISBIN, hvilket også omfatter videreoverførsler med henblik på national sikkerhed. Databeskyttelsesrådet opfordrer Kommissionen til yderligere at præcisere retsgrundlaget samt de databeskyttelsesgarantier og -betingelser, som ABIN og de øvrige medlemmer af SISBIN skal tage i betragtning, inden de videregiver personoplysninger til udenlandske partnere til nationale efterretningsformål.
- (103) Databeskyttelsesrådet bemærker også, at Kommissionen ikke tog stilling til eksistensen af internationale aftaler indgået mellem Brasilien og tredjelande eller internationale organisationer i sin tilstrækkelighedsvurdering. Da LGPD ikke indeholder bindende lovgivning ud over de generelle databeskyttelsesprincipper, kan sådanne aftaler indeholde specifikke bestemmelser om international overførsel af personoplysninger, som ABIN eller de øvrige SISBIN-medlemmer er i besiddelse af, til tredjelande. Databeskyttelsesrådet mener, at indgåelsen af bilaterale eller multilaterale aftaler med tredjelande med henblik på national efterretning sandsynligvis vil påvirke de gældende retlige rammer for databeskyttelse.
- (104) Databeskyttelsesrådet opfordrer derfor Kommissionen til at præcisere, om der findes sådanne internationale aftaler til nationale efterretningsformål, og til at vurdere deres potentielle indvirkning på beskyttelsesniveauet for personoplysninger, der overføres fra EØS til Brasilien, i forhold til den primært vurderede retlige ramme for databehandling til nationale efterretningsformål.

3.2.4 Tilsyn og klagemuligheder

- (105) I udkastet til afgørelse om tilstrækkeligheden præsenteres forskellige organer, der skal føre tilsyn med de brasilianske nationale sikkerhedsmyndigheders aktiviteter, navnlig i) den udøvende magt, ii) den lovgivende magt, iii) ANPD, og iv) den dømmende magt. Med hensyn til ANPD minder Databeskyttelsesrådet om de overvejelser og konklusioner, der er gjort i afsnit 3.1.4 i denne udtalelse, og som også er gældende her.
- (106) Ifølge udkastet til afgørelse er regeringsrådets kammer for eksterne forbindelser og nationalt forsvar ansvarligt for tilsynet med gennemførelsen af det nationale efterretningspoliti, og kontoret for institutionel sikkerhed er ansvarligt for at koordinere de føderale efterretningstjenesters aktiviteter. Databeskyttelsesrådet bemærker, at denne kontrol kun vedrører sikringen af, at de mål, der skal nås med efterretningssystemet, er opnået, men ikke omfatter undersøgelses- eller sanktionsbeføjelser og ikke dækker den faktiske behandling af personoplysninger.
- (107) Det er faktisk det fælles udvalg for kontrol med efterretningsaktiviteter (CCAI) (den lovgivende myndighed), der skal udøve kontrol med efterretningsaktiviteter, herunder deres legitimitet og effektivitet. Databeskyttelsesrådet glæder sig over, at CCAI's struktur og beføjelser er blevet styrket, hvilket har øget gennemsigtigheden af dets aktiviteter og gjort det muligt for organet at udøve passende kontrol, f.eks. ved at foretage efterfølgende gennemgang, revisioner og kontrol af igangværende operationer. Databeskyttelsesrådet bemærker også med tilfredshed, at CCAI kan behandle registreredes klager som led i sin kompetence til at undersøge klager over krænkelse af grundlæggende rettigheder og garantier.

- (108) Retsvæsenets kompetence til at behandle sager anlagt af borgere mod offentlige myndigheder er et positivt aspekt, især da det giver mulighed for retsligt tilsyn med aktiviteter, der udføres i den nationale sikkerheds navn, og sikrer overholdelse af bl.a. forfatningsmæssige rettigheder (herunder retten til databeskyttelse) og LGPD. Databeskyttelsesrådet noterer sig med tilfredshed, at der er mulighed for appel via den føderale højesteret og i sidste ende via Den Interamerikanske Menneskerettighedsdomstol.
- (109) Det er Databeskyttelsesrådets opfattelse, at de registrerede i forbindelse med nationale efterretningsaktiviteter får i) de rettigheder, der er nedfældet i LGPD (som følge af den føderale højesterets afgørelse af 15. september 2022), ii) retten til indsigt i og berigtigelse af personoplysninger gennem den forfatningsmæssige klagemulighed i Habeas Data samt iii) retten til kompensation for materielle og ikkematerielle skader.
- (110) Databeskyttelsesrådet glæder sig over disse rettigheder og over, at de kan gøres gældende gennem retslige og administrative mekanismer, navnlig CCAI, samt over, at disse klagemuligheder er tilgængelige for alle personer, uanset nationalitet.

4. GENNEMFØRELSE OG OVERVÅGNING AF UDKASTET TIL AFGØRELSE

- (111) Med hensyn til overvågning og revision af udkastet til afgørelse bemærker Databeskyttelsesrådet, at følgende gælder i henhold til EU-Domstolens praksis: "Henset til den omstændighed, at det beskyttelsesniveau, som et tredjeland sikrer, kan ændre sig, påhviler det endvidere Kommissionen efter vedtagelse af en afgørelse i henhold til [databeskyttelsesforordningens artikel 45] at undersøge med regelmæssige mellemrum, om konstateringen vedrørende det tilstrækkelige beskyttelsesniveau, som er sikret i det pågældende tredjeland, stadig er faktisk og retligt begrundet. En sådan undersøgelse skal under alle omstændigheder foretages, når oplysninger bevirker, at der opstår tvivl i denne henseende"⁸¹.
- (112) Databeskyttelsesrådet bemærker, at evalueringen af konstateringen af et tilstrækkeligt beskyttelsesniveau vil finde sted mindst hvert fjerde år i overensstemmelse med artikel 45, stk. 3, i databeskyttelsesforordningen⁸².
- (113) Databeskyttelsesrådet glæder sig over, at det i udkastet til afgørelse i betragtning 230 fastsættes, at Databeskyttelsesrådet deltager i det møde, der organiseres mellem Kommissionen og de brasilianske myndigheder, hvor det skal gennemgås, hvordan afgørelsen om tilstrækkeligheden fungerer. Med hensyn til den praktiske inddragelse af Databeskyttelsesrådet og dets repræsentanter i forberedelsen og gennemførelsen af fremtidige periodiske evalueringer gentager Databeskyttelsesrådet, at al relevant dokumentation, herunder korrespondance, bør deles skriftligt med Databeskyttelsesrådet i tilstrækkelig god tid inden evalueringerne.

På Det Europæiske Databeskyttelsesråds vegne

Formand

⁸¹ Domstolens dom i Schrems I-sagen, præmis 76. Se også artikel 3, stk. 4, i udkastet til afgørelse.

⁸² Se betragtning 229 og artikel 3, stk. 4, i udkastet til afgørelse.

(Anu Talus)