FAST LTA

Een kritische feitencheck over dataveiligheid

US Cloud Act, FISA en het Data Privacy Framework

Sinds: maart 2025

Executive Summary

De CLOUD Act en FISA 702 geven Amerikaanse autoriteiten vergaande toegang tot Europese gegevens die zijn opgeslagen in Amerikaanse clouds. Dit is in strijd met de GDPR en vormt een aanzienlijk risico voor Europese bedrijven. Overtredingen van de GDPR kunnen immers boetes opleveren tot 20 miljoen euro of 4% van de wereldwijde jaaromzet.

Het EU-VS Data Privacy Framework (DPF) was bedoeld om rechtszekerheid te creëren, maar na het aantreden van Donald Trump werd het centrale toezichthoudende orgaan van het DPF - de Privacy and Civil Liberties Oversight Board - feitelijk handelingsonbekwaam gemaakt door het ontslag van verschillende leden. Bovendien is de hele architectuur van de DPF voornamelijk gebaseerd op een uitvoerend bevel van Joe Biden, dat Donald Trump op elk moment kan intrekken.

De situatie vereist dat bedrijven onmiddellijk in actie komen: Een systematische inventarisatie van alle gegevensstromen naar Amerikaanse clouddiensten en een op risico's gebaseerde analyse van de beschermingsbehoeften zijn essentieel. De migratie van zeer gevoelige gegevens naar on-premises oplossingen in combinatie met het gebruik van end-to-end encryptie met client-side sleutelbeheer wordt aanbevolen.

De huidige politieke ontwikkelingen in de VS maken duidelijk dat Europese bedrijven hun digitale soevereiniteit moeten versterken en zich minder afhankelijk moeten maken van geopolitieke ontwikkelingen.

Trans-atlantische datatransfers in crisis

De internationale overdracht van persoonsgegevens is een dagelijkse noodzaak geworden in de geglobaliseerde economie. Elke dag brengen bedrijven enorme hoeveelheden gegevens over de landsgrenzen heen, of het nu gaat om communicatie binnen een groep, cloud computing of internationale diensten.

Economische belangen, gegevensbeschermingsvereisten en nationale veiligheidsinspanningen botsen echter vaak met elkaar bij deze gegevensoverdrachten. Het potentieel voor conflicten is vooral duidelijk in de trans-Atlantische relatie, waar de GDPR botst met de vergaande bevoegdheden van de Amerikaanse veiligheidsautoriteiten.

Duidelijke wettelijke regels waren bedoeld om dit conflict op te lossen, maar zijn tot op heden keer op keer mislukt. Onlangs nog, na het baanbrekende Schrems II-arrest van het Europees Hof van Justitie, moesten de randvoorwaarden voor internationale gegevensoverdracht fundamenteel worden gereorganiseerd. Het gegevensbeschermingskader werd in 2023 van kracht, maar of het zal voldoen aan de eisen van het EHJ is allesbehalve zeker.

De juridische onzekerheid heeft concrete gevolgen voor bedrijven, die nu gedwongen zijn om hun trans-Atlantische gegevensoverdrachten kritisch te bekijken. Deze situatie zorgt niet alleen voor technische en organisatorische uitdagingen, maar ook voor aanzienlijke economische risico's voor internationaal opererende bedrijven.

Wat betekent de US CLOUD Act voor Europese bedrijven?

De Clarifying Lawful Overseas Use of Data (CLOUD) Act, die in maart 2018 werd aangenomen, geeft Amerikaanse rechtshandhavingsinstanties toegang tot alle bedrijfs- en klantgegevens van cloud- en communicatieproviders - ongeacht waar de gegevens fysiek zijn opgeslagen. Dit geldt voor alle Amerikaanse bedrijven en hun dochterondernemingen, inclusief grote cloudproviders zoals AWS, Google Cloud en Microsoft Azure.

Zelfs gegevens die zijn opgeslagen in datacenters in de EU zijn niet beschermd tegen toegang door de autoriteiten, wat betekent dat handelsgeheimen, intellectueel eigendom en andere gevoelige informatie kunnen worden ingezien door Amerikaanse autoriteiten.

De CLOUD Act is uitsluitend bedoeld voor de vervolging van en het onderzoek naar ernstige misdrijven. Hiervoor is een gerechtelijk huiszoekingsbevel nodig en alleen gerichte individuele zoekopdrachten zijn toegestaan. Ondanks deze beperkingen betekent het al een fundamentele inbreuk op de Europese gegevenssoevereiniteit.

Nog ernstiger dan de bevoegdheden die door de CLOUD Act worden verleend, zijn de mogelijkheden die kunnen worden ontleend aan Sectie 702 van de Foreign Intelligence Surveillance Act (FISA 702).

Hoe ver reiken de controlebevoegdheden van FISA 702?

Artikel 7 van het EU-Handvest van de Grondrechten stelt ondubbelzinnig: “Een ieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie“[1]. Deze formulering stelt een alomvattend recht op bescherming vast, dat wordt opgevat als een fundamenteel mensenrecht en dat niet voorziet in beperkingen.

Dit staat in contrast met de Amerikaanse rechtspraktijk. Het is waar dat het Vierde Amendement van de Amerikaanse Grondwet beschermt tegen onredelijke huiszoekingen en inbeslagnames. Deze bescherming geldt echter alleen voor Amerikaanse burgers.

Niet-Amerikaanse burgers kunnen op grote schaal bespioneerd worden in het belang van de nationale veiligheid. De Foreign Intelligence Surveillance Act, die in 1978 werd aangenomen en een kader biedt voor de buitenlandse inlichtingen- en contraspionageactiviteiten van de Verenigde Staten, regelt de omvang van de bevoegdheden van de inlichtingendiensten.

In 2008 werd FISA Sectie 702 (FISA 702) goedgekeurd als onderdeel van de USA PATRIOT Act. Sindsdien hebben de inlichtingendiensten geen gerechtelijk bevel meer nodig om toegang te krijgen tot gegevens van aanbieders van elektronische communicatiediensten, op voorwaarde dat het doelwit van de gegevenstoegang geen Amerikaans staatsburger is en zich buiten de VS bevindt[2].

De onthullingen van de surveillance- en spionageaffaire die Edward Snowden in 2013 in gang zette, lieten zien hoe ver de Amerikaanse inlichtingendiensten gaan. Amerikaanse bedrijven zoals Microsoft, Google, Apple en Facebook verleenden de inlichtingendiensten toegang tot live communicatie en opgeslagen informatie als onderdeel van het PRISM-programma[3].

In 2024 werden de bevoegdheden van FISA opnieuw uitgebreid door aanbieders van elektronische communicatiediensten (ECSP's) opnieuw te definiëren. In de versie van 2008 omvatten ECSP's alleen bedrijven zoals Google, Meta en AT&T die de toegang tot communicatie direct faciliteren of mogelijk maken. Sinds 2024 omvat de term elke organisatie of persoon die toegang heeft tot apparaten waarop communicatie wordt opgeslagen of via welke communicatie wordt verzonden. Beperkte uitzonderingen bestaan alleen voor restaurants, hotels, woningen en gemeentelijke voorzieningen[4]. Voor Europese gebruikers van Amerikaanse clouddiensten betekent dit dat hun gegevens vrijwel onbeperkt kunnen worden gecontroleerd.

De belangrijkste verschillen tussen de CLOUD ACT en FISA 702

FISA 702 en de CLOUD Act verschillen fundamenteel in hun doelen en bevoegdheden:

CLOUD Act	FISA 702
Gebruikt voor strafrechtelijke vervolging	Inlichtingendoeleinden
Onderhevig aan gerechtelijke controle	Geen gerechtelijke controle
Staat alleen gerichte individuele zoekopdrachten toe	Massasurveillance mogelijk

Welke bescherming biedt het Data Privacy Framework (DPF)?

De overdracht van persoonsgegevens tussen de Europese Unie en de Verenigde Staten kent een complexe geschiedenis. In 2000 werd de eerste "Safe Harbor" overeenkomst gesloten.[5] Dit was bedoeld om ervoor te zorgen dat Amerikaanse bedrijven voldoen aan strenge Europese normen voor gegevensbescherming wanneer ze gegevens van EU-burgers verwerken. Na de onthullingen van Edward Snowden in 2013 over massasurveillance door de Amerikaanse inlichtingendiensten werd het echter duidelijk dat Safe Harbour niet voldeed aan zijn beschermende doel. Het Europese Hof van Justitie verklaarde de overeenkomst ongeldig in 2015[6].

Als opvolger werd in 2016 het “Privacy Shield” geïntroduceerd. Maar zelfs deze overeenkomst kon de fundamentele problemen niet oplossen. De Oostenrijkse activist voor gegevensbescherming Max Schrems spande met succes een rechtszaak aan tegen het Privacy Shield. Het Europees Hof van Justitie volgde zijn argument en vernietigde ook deze overeenkomst in 2020. Het Hof hekelde met name het feit dat Amerikaanse inlichtingendiensten nog steeds te vergaande toegangsrechten hadden tot Europese gegevens en dat EU-burgers zich hier niet effectief tegen konden verdedigen[7].

Het Data Privacy Framework, dat sinds juli 2023 van kracht is, probeert de zwakke punten van de vorige regelgeving te verhelpen. Centraal staat een fundamentele reorganisatie van de manier waarop Amerikaanse autoriteiten met Europese gegevens mogen omgaan. President Biden vaardigde hiervoor in oktober 2022 een speciaal uitvoeringsbevel (14086) uit. De Privacy and Civil Liberties Oversight Board (PCLOB) speelt hierin een centrale rol en fungeert als onafhankelijk toezichthoudend orgaan om te controleren of Amerikaanse diensten zich daadwerkelijk houden aan de wetten en verplichtingen op het gebied van gegevensbescherming. De PCLOB houdt in het bijzonder toezicht op de naleving van de vereisten van Executive Order 14086, die de verwerking van persoonsgegevens uit de EU regelt[8].

De nieuwe regels bepalen dat Amerikaanse autoriteiten alleen toegang hebben tot Europese gegevens als dit absoluut noodzakelijk is voor specifieke, legitieme veiligheidsdoeleinden. Een belangrijke vernieuwing in dit verband is het tweeledige rechtsbeschermingsmechanisme. De “Civil Liberties Protection Officer” werd opgericht als eerste contactpunt. Dit is een persoon die ervoor moet zorgen dat de Amerikaanse inlichtingendiensten de grondrechten naleven en de privacy respecteren[9].

Het Data Protection Review Court (DPRC) werd opgericht als tweede belangrijke instantie. Deze rechtbank bestaat uit ervaren advocaten die geen lid zijn van de Amerikaanse overheid. Ze hebben uitgebreide bevoegdheden en kunnen ook geheime documenten van de inlichtingendiensten inzien en bindende bevelen geven, zoals het verwijderen van onrechtmatig verzamelde gegevens.

Dit panel beoordeelt de beslissingen van de CLPO als het wangedrag van de inlichtingendiensten vaststelt. De rechters in dit panel worden benoemd door de Attorney General in overleg met de Secretary of Commerce en de Director of National Intelligence[10]. Concreet betekent dit dat rechters, die zijn goedgekeurd door het hoogste hoofd van de Amerikaanse geheime diensten, de praktijken van deze diensten moeten veroordelen.

Amerikaanse bedrijven die persoonsgegevens uit de EU willen verwerken, kunnen zichzelf vrijwillig certificeren bij het Amerikaanse ministerie van Handel onder het Data Privacy Framework. Om gecertificeerd te worden, moeten bedrijven publiekelijk toezeggen de DPF-principes na te leven, d.w.z. dat ze ook moeten voldoen aan de Europese normen voor gegevensbescherming. Deze belofte is vervolgens afdwingbaar onder de Amerikaanse wetgeving. De naleving van de verplichtingen wordt gecontroleerd door het Amerikaanse ministerie van Handel[11].

Als EU-burgers vermoeden dat hun gegevens worden misbruikt, kunnen ze contact opnemen met de bevoegde toezichthoudende autoriteiten voor gegevensbescherming. De klachtenprocedure voorziet in verschillende rechtsmiddelen, die door het Europees Comité voor gegevensbescherming (EDPB) worden geregeld in overeenkomstige procedureregels[12].

Hoe veilig is de DPF?

Het EU-VS Data Privacy Framework is de derde poging om tot een gemeenschappelijke noemer te komen in het trans-Atlantische gegevensbeschermingsbeleid. Hoewel de Europese Commissie voldoende vooruitgang ziet in de nieuwe beschermende maatregelen voor inlichtingensurveillance en het pas opgerichte Data Protection Review Court, is er al aanzienlijke weerstand.

Het Europees Parlement heeft een bijzonder kritisch standpunt ingenomen en heeft in mei 2023 in een opmerkelijk duidelijke resolutie (306 stemmen voor, 27 tegen) zijn fundamentele bezorgdheid geuit over de juridische conformiteit van het kader[13]. Deze scepsis wordt gedeeld door activisten voor gegevensbescherming zoals Max Schrems en zijn organisatie NOYB, die de nieuwe overeenkomst zien als een oppervlakkig herziene versie van het mislukte Privacy Shield en al juridische stappen voorbereiden[14].

Sinds het aantreden van Donald Trump op 20 januari 2025 is de bezorgdheid enorm toegenomen. De regering Trump ontsloeg drie Democratische leden van de Privacy and Civil Liberties Oversight Board (PCLOB) slechts een paar dagen na haar aantreden eind januari. Omdat de PCLOB ten minste drie actieve leden nodig heeft om een quorum te hebben, kan het centrale toezichthoudende orgaan voor de naleving van de gegevensbeschermingsregels sindsdien niet meer functioneren.

Critici waarschuwen dat dit slechts het begin kan zijn van een algehele uitholling van het kader voor gegevensbescherming. Het Data Protection Review Court heeft een nog zwakkere rechtsgrondslag dan de PCLOB, en Trump heeft al aangekondigd dat hij alle orders van Joe Biden zal herzien. De juridische architectuur van het kader is grotendeels gebaseerd op Biden‘s Executive Order 14086, die Trump met een eenvoudig tegenbevel zou kunnen intrekken. Dit zou de hele reeks regels praktisch van de ene dag op de andere van hun rechtsgrondslag beroven.

Wat als de DPF het begeeft?

Een mislukking van het DPF zou verstrekkende gevolgen hebben voor de trans-Atlantische gegevensuitwisseling. Bedrijven die voor hun dagelijkse bedrijfsactiviteiten afhankelijk zijn van Amerikaanse clouddiensten en digitale diensten zouden worden getroffen. De gevolgen zouden vooral merkbaar zijn voor kleine en middelgrote ondernemingen.

Voor medische praktijken en zorgverleners betekent dit dat gevoelige patiëntgegevens die momenteel zijn opgeslagen in Amerikaanse cloudsystemen zoals AWS onmiddellijk zouden moeten worden overgezet naar alternatieve systemen. Ingenieursbureaus en productiebedrijven zouden ook hun vertrouwelijke ontwerpgegevens en ontwikkelingsdocumenten opnieuw moeten beveiligen. Belastingadviseurs en accountants, die hun klant- en financiële documenten voorheen misschien in Dropbox hebben opgeslagen, zouden voor de uitdaging komen te staan om deze volledig te migreren.

Een alternatief zou zijn om standaard contractuele clausules of bindende bedrijfsregels op te stellen. Aangezien het echter de vraag is of deze zelfs in staat zijn om het juridische dilemma tussen de GDPR en de vereisten van de Amerikaanse autoriteiten op te lossen, zouden ze in het beste geval als een overgangsoplossing moeten fungeren. Bovendien is dit proces niet alleen tijdrovend en kostenintensief, maar vereist het ook aanzienlijke juridische expertise. Vooral kleine en middelgrote ondernemingen (KMO's) en startende bedrijven zouden zwaar worden getroffen door deze extra administratieve en financiële lasten.

Veel Europese bedrijven zouden hun hele IT-infrastructuur moeten herzien en mogelijk volledig reorganiseren. Dit betreft niet alleen de voor de hand liggende cloudopslagdiensten, maar ook minder voor de hand liggende diensten zoals marketingtools, CRM-systemen of communicatieplatforms. De bijbehorende kosten voor migratie, training en procesaanpassing kunnen aanzienlijk zijn.

Bovendien kan niet-naleving van de GDPR-vereisten in het geval van ongeautoriseerde overdracht van persoonlijke gegevens aan ontvangers in een derde land leiden tot zware boetes tot €20 miljoen of 4% van de wereldwijde jaaromzet, afhankelijk van welke hoger is[15].

Concrete onmiddellijke maatregelen voor versterking van de gegevensbeveiliging

Vanwege de kwetsbaarheid van de bestaande regelgeving moeten bedrijven concrete maatregelen nemen om kritieke gegevens te beveiligen.

1. Ten eerste is een systematische inventarisatie van gegevensstromen essentieel. Dit begint met een gedetailleerde inventarisatie van alle gegevens die worden overgedragen aan Amerikaanse clouddiensten. Het is belangrijk om gevoelige persoonlijke gegevens apart te categoriseren in overeenstemming met de GDPR en om te documenteren waar deze gegevens worden opgeslagen, wie er toegang toe heeft en voor welk doel ze worden verwerkt. Net zo relevant is de uitgebreide documentatie van de gebruikte cloudinfrastructuur, inclusief alle API's, integraties met derden en de fysieke locaties van de servers.

2 De tweede belangrijke stap is het uitvoeren van een risicogebaseerde analyse van de beschermingsbehoeften. Deze analyse begint met het identificeren van potentiële bedreigingen voor de gegevens, zoals toegang tot overheidsgegevens, aanvallen op de toeleveringsketen of interne bedreigingen. Vervolgens moeten de beschermingsvereisten van de gegevens worden bepaald, waarbij een onderscheid wordt gemaakt tussen categorieën als normaal, hoog en zeer hoog, rekening houdend met mogelijke schade (financieel, reputatieverlies, aantasting van grondrechten). De risicobeoordeling wordt afgesloten met een risicomatrix die de waarschijnlijkheid van het optreden van bedreigingen combineert met de potentiële omvang van de schade om het risiconiveau zichtbaar te maken en prioriteiten te stellen.

3 Ten derde is de implementatie van verbeterde technische beveiligingsmaatregelen voor gegevens met hoge beschermingsvereisten essentieel. Dit omvat het gebruik van end-to-end versleuteling met client-side sleutelbeheer om ervoor te zorgen dat cloud providers geen toegang hebben tot de gegevens. Daarnaast moeten ‚zero trust'-architecturen met authenticatie op meerdere niveaus en netwerken met microsegmenten worden geïmplementeerd om de toegang tot kritieke gegevenspools te isoleren en te controleren. Georedundante back-ups in Europese high-security datacenters, idealiter gecertificeerd volgens ISO 27001 en C5, zijn noodzakelijk voor betrouwbare gegevensbescherming.

4 Ten vierde zijn organisatorische aanpassingen nodig om crises te voorkomen en het reactievermogen te versterken. Dit omvat het opzetten van een noodplan met een taskforce-team dat duidelijke verantwoordelijkheden definieert voor het implementeren van exitstrategieën in het geval van wijzigingen in het wettelijke kader. Regelmatige trainingsprogramma's voor werknemers over onderwerpen als veilig programmeren, phishing-detectie en gegevensbeschermingsconform gebruik van samenwerkingstools zijn essentieel om het bewustzijn en de competentie op het gebied van gegevensbeveiliging te vergroten. Daarnaast moeten red teaming-oefeningen worden uitgevoerd om gesimuleerde cyberaanvallen te ervaren en de verdedigingsmogelijkheden tegen geavanceerde bedreigingen te testen.

5 Tot slot is strategische toekomstplanning essentieel voor veerkracht en digitale soevereiniteit op de lange termijn. Dit omvat het evalueren van hybride cloudmodellen waarbij gevoelige kerngegevens in lokale oplossingen of privéclouds blijven, terwijl minder kritieke workloads kunnen worden uitbesteed aan Amerikaanse cloudservices.

Conclusie

De laatste ontwikkelingen in de VS, met name de verlamming van de Privacy and Civil Liberties Oversight Board door de regering-Trump eind januari 2025, hebben de toch al kwetsbare structuur van het dataprivacyraamwerk fundamenteel door elkaar geschud. Deze situatie dwingt Europese bedrijven om onmiddellijk actie te ondernemen om hun gegevensoverdrachten in overeenstemming te brengen met de wet en mogelijke schendingen van de GDPR te voorkomen.

Een belangrijke aanbeveling voor actie is de consequente ontwikkeling van een on-premises strategie voor gevoelige persoonlijke gegevens. Concreet betekent dit dat bedrijven eerst een uitgebreide risicoanalyse van hun bestaande gegevensstromen moeten uitvoeren en kritieke gegevensvoorraden moeten identificeren. Tegelijkertijd moet een begin worden gemaakt met de ontwikkeling van een aparte, controleerbare infrastructuur voor bijzonder gevoelige gegevens. Deze transformatie moet worden gezien als een strategisch proces dat geleidelijk en volgens duidelijke prioriteiten verloopt.

Voor minder gevoelige gegevens kunnen Europese cloudalternatieven of hybride cloudoplossingen worden overwogen. Standaard contractuele clausules (SCC's) zijn een geschikte tussenoplossing, maar deze moeten worden geflankeerd door aanvullende technische en organisatorische maatregelen. Gezien de dreiging van GDPR-boetes en mogelijke reputatieschade zijn de bijbehorende investeringen zeker gerechtvaardigd.

De huidige politieke situatie in de VS benadrukt de urgentie van deze maatregelen. De aankondiging van Trump dat hij alle orders van Biden zal herzien, kan de hele DPF-constructie doen instorten. Bedrijven zouden deze gedwongen transformatie echter moeten zien als een kans om hun digitale soevereiniteit terug te winnen en minder afhankelijk te worden van geopolitieke ontwikkelingen. Het opzetten van een eigen, controleerbare infrastructuur voor gevoelige gegevens is niet alleen een juridische noodzaak, maar ook een strategisch voordeel in het steeds complexer wordende internationale dataverkeer.

Als specialist in de veilige opslag van gevoelige gegevens bieden wij u een uitgebreide risicocheck met onze experts. Samen analyseren we uw bestaande gegevensstromen naar Amerikaanse cloudservices, identificeren we kritieke gebieden en ontwikkelen we op maat gemaakte oplossingen op locatie die uw gegevens betrouwbaar beschermen tegen ongewenste toegang door Amerikaanse autoriteiten.

Referenties

1 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12012P/TXT

2 https://www.fbi.gov/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702

3 https://de.wikipedia.org/wiki/PRISM

4 https://cdt.org/insights/the-secret-law-key-that-could-unlock-a-pandoras-box-of-uncurtailed-government-surveillance/

5 https://eur-lex.europa.eu/eli/dec/2000/520/oj/eng

6 https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

7 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62018CJ0311

8 https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

9 https://www.robin-data.io/datenschutz-akademie/news/eu-us-data-privacy-framework

10 https://esb-data.de/biden-erlass-zum-eu-us-data-privacy-framework/

11 https://www.dataprivacyframework.gov/Program-Overview

12 https://www.datenschutz-mv.de/datenschutz/publikationen/EU%E2%80%93US_DPF/

13 https://www.hunton.com/privacy-and-information-security-law/european-parliament-adopts-eu-u-s-data-privacy-framework-resolution

14 https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

15 https://www.datenschutz.org/dsgvo-bussgeld/

FAST LTA

FAST LTA
Rüdesheimer Str. 11
80686 München
info@fast-lta.de
www.fast-lta.de

Design,
Entwicklung
und Support
in **Deutschland**

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**