ISSA DC
August 17, 2023

US Biden EO 14086 DATA PRIVACY FRAMEWORK: IS IT EU ADEQUATE?

Linda V. Priebe, JD, CIPP/E
Co-Chair, Government, Regulatory & Compliance Practice Group
Culhane Meadows, PLLC
Washington, DC
lpriebe@cm.law

CULHANE MEADOWS PLLC

US Biden EO 14086 DATA PRIVACY FRAMEWORK: IS IT EU ADEQUATE?

Linda V. Priebe, JD, CIPP/E,
Partner & Co-Chair, Government, Regulatory & Compliance Practice Group
Culhane Meadows PLLC, Washington, DC, USA, email: lpriebe@cm.law

- **Culhane Meadows EU-U.S. data privacy/protection compliance & transactions DC, 2014-present**
  - **CIPP/E certified Int'l Assoc of Privacy Professionals,** 2016-present
  - **Drafted/Negotiated 500+ GDPR & CCPA/CPRA data privacy/protection agreements/addenda**

- **Former DGC & Agency Ethics Official, White House Office of Drug Policy, DC,** 1999-2013
  - **Ethics &Compliance Program Management & Operation including children's privacy, & social & digital media compliance**

- **Co-Chair & Vice Chair, ABA ILS Privacy, Cybersecurity & Digital Rights Committee** 2016-present

- **ABA President's Cybersecurity Legal Task Force** 2022-present

- **Adjunct Professor, U.S. & EU Data Privacy & Cybersecurity, Fordham Law School, Masters Program in Corporate Compliance,** 2021-present

CULHANE MEADOWS PLLC

EU-U.S. Data Access/Transfers/Flows Basic Legal Concepts

GDPR= much more protective of individs **located in EU** (res/cit not req'd) **than U.S.**

- **Fund'l Human Right**
- **Fines** up to **4% Gross Sales/Proceeds** (versus profits) **or 20 Mill Euros (whichever is higher) EX: Irish DPC v. FB/Meta $1.3 Bill; Norway $96K/day**
- **Worse EU-US PD Access/Transfers/Flows must use & comply with an EU GDPR legal adequacy mechanism** like SCCs, BCRs, Compliance Framework (EU-US Priv Shield) **OR data access/transfers/ flows can be cut off/suspended by EU regulators EX: Irish DPC v. FB/Meta w/in 5 mos**

CULHANE MEADOWS PLLC

EU-U.S. Data Access/Transfers GDPR Broad Definitions

- **Protected Persons =** consumers **+** biz POCs in pro capacity **+** employees **+** temp workers **+** K'tors **located in EU/EEA/Switzerland/UK even in workplace + using employer's equipment.**
- **PI/PD = Any info** alone **or** in combo **capable** of being used to **ID an individual** (w/o attempt to actually ID individ)
  - **=** dynamic **IP addresses** & **device IDs**
- **Transfers/Flows = access EU PD from devices** located outside the EU/EEA/UK/Switz
- **GDPR Extraterritorial Jurisdiction Triggered** by U.S. Companies **when**
- **Workforce** member (**1+**) **OR Equipment** (inc'g computers**) OR Offices in EU/EEA/UK/Switzerland OR**
  - **Offering Goods/Services** [online] to **Persons in** EU/EEA/UK/Switzerland
  - **Monitoring** [local] **behavior of Persons in** EU/EEA/UK/Switzerland =
    - **Tracking online or**
    - **Profiling to predict preferences = Digital Ads & Google & FB Analytics**

- **GDPR requires EU approved int'l data transfer legal adequacy mechanism for EU-US PD access/transfers/flows** (essentially GDPR equivalent)**;** i.e. SCC, BCR, EU-U.S. framework (**former EU-U.S. Privacy Shield/Biden DPF**)

CULHANE MEADOWS PLLC

Schrems II = Max Schrems vs Facebook/Meta

- **2013 Schrems** (law student now Lawyer) **filed complaint w/ Irish DPC v. Facebook re: potential US law enforcement (NSA FISA) access to his PD on/in Facebook**
- **2015 CJEU Schrems I: US-EU Safe Harbor** compliance framework for EU PD access /transfers/flows to/in U.S. **= invalid + SA's can suspend PD trans/access/flows** .
- **2015 Schrems resubmitted complaint v FB to Irish DPC** to enforce Schrems I.
- **2016 EC** deemed updated **EU-U.S. Privacy Shield** compliance framework **adequate** for EU-US PD access/transfers/flows
- **2020 CJEU Schrems II: Struck down EU-U.S. Privacy Shield** for EU-U.S. data access/transfers/flows **due to USG access per FISA 702 & EO 12333**
  - **Req's TIAs + Supp Sec Measures Ever Participated in TIA? Raise Your Hand!**
- **Watch This Space: Schrems III is expected**

CULHANE MEADOWS PLLC

Biden EO 14086: U.S. Signals Intelligence Activities For EU-U.S. Data Access/Transfers – Overview

- **Updates EU-US Privacy Shield for US orgs self-cert GDPR compliance** re: EU-US data access/transfers/flows
- Designed to **resolve Schrems II** concerns re: breadth of **US Intel Agencies access to EU PD** (via electronic communications) under **FISA 702** (w/in US = FISA Ct) & **EO 12333** (outside US – no FISA Ct) by **providing more privacy protections to Foreign Persons**.
- **FISA 702 still more privacy protections for US Persons** than Biden EO provides Foreign Persons, but **both allow USG to target persons who present no threat to US Nat'l Security.**
- **FISA 702 C Reauth** pending **- Pres Intell Adv Bd 13 Recs**

CULHANE MEADOWS PLLC

Biden EO 14086: U.S. Signals Intelligence Activities For EU-U.S. Data Access/Transfers – Overview 2

Under Biden EO U.S. Intel agencies permitted to conduct **electronic surveillance for foreign intel** ("signal activities") **only when:**

- **necessary & proportionate** (Int'l law definition rejected by DOJ) to advance 1 of 12 "**legitimate**" U.S. nat'l security objectives "**validated**" by the Civil Liberties Protection Officer of the U.S. Director of National Intelligence (**CLPO**);
- "privacy and civil liberties of **all persons**, **regardless of nationality or country of residence"** is taken into consideration **& all available less intrusive means;**
- subject to **new data minimization, sharing & retention limits.** (Note post data collection limits)
- BUT **BULK** Surveillance **unlimited by "legitimate objectives" & w/o warrant still permitted** (may sweep up U.S. Persons + Foreign Persons)

CULHANE MEADOWS PLLC

Biden EO 14086: PD Collection Permitted ONLY for 12 Legitimate National Security Objectives

Assess capabilities/intentions/activities of:

- **Foreign Gov/Mil/Faction/Polit Orgs**
- **Int'l Terror Orgs**
- **Global Sec threats** = climate, pub health, humanitarian, polit instability, geographic rivalry

Protect against:

- Foreign **Military** capabilities & activities
- **Terror/HostageTaking** for US & other For Govs/Orgs/Persons
- Foreign Gov **Espionage/Sabotage/Assassination**/Other Intel Activities
- Devel/Possess/Proliferation **of WMDs**
- **Cyber threats/Malicious Cyber Activity**
- Threats to US or Allied **Personnel**
- **Crime** = illicit finance & sanctions evasion
- Physical/electronic threats to **Election Integrity/Polit Processes/Gov Prop/US Infrastructure**

Advance collection/capabilities/activities to further above

Note: Most EU Member States not as transparent re: own collection of Intel Data

CULHANE MEADOWS PLLC

Biden EO 14086: Redress Mechanism

EO creates a **2-tiered system to review and resolve complaints** from individuals in the EU about U.S. signals intelligence activities:

1. **CLPO** (Civil Liberties Protection Officer of the U.S. Director of National Intelligence) is required to **investigate complaints** (independent from the Director of National Intelligence) to determine **whether the EO safeguards** or **other U.S. laws were violated** and if so, **determine** an **appropriate binding remedy**.

2. New **Data Protection Review Court** created by the **U.S. DOJ** to provide independent **and binding review** of the **CLPO's decisions**.

The **UK has also in** process to review legal adequacy of the Biden EO for UK-U.S data access/transfers/flows under the UK GDPR.

CULHANE MEADOWS PLLC

Biden EO 14086: USG IC Implementation

7/3/23 **US** **ODNI** releases IC **implementation policies and procedures** for:

- **FBI**
- **NSA**
- **CIA**
- **DHS**
- **DEA**
- **ODNI**
- **Office of National Security Intelligence (ONSI)**
- **National Reconnaissance Office (NRO)**
- **Coast Guard**
- **DOE**
- **State**
- **Treasury**

https://lnkd.in/eqvc8iiB

CULHANE MEADOWS PLLC

EC U.S. Adequacy Decision 7/10/23

Biden EO 14086 + U.S. DOJ Data Protection Review Court Regulations **= "essentially equivalent" to GDPR compliance for EU-U.S. PD access/transfers/flows** ("EU-U.S. Data Privacy Framework")

Resolves Schrems II US PD surveillance concerns under EO 12333 U.S. signals intelligence activity & FISA 702 "bulk" data collection, without effective redress required by EU fundamental human rights

-**Limits U.S. Intel Agencies & Signals Intel access to PD "necessary & proportionate" to protect Natl Sec**

-**Provides "effective redress rights" to EU individuals** (BUT EDPB Opinion + Info Note)

U.S. DOC Voluntary self-cert w/ 1yr renewal (former renewal 2 yrs) **+ FTC enforcement** (DOT for airlines & regulated transportation services)

GDPR equivalent DP Obligations: Transparency; Data min & accuracy; Purpose limitation (specified Nat'l Sec purposes & Consent for new purposes); Enhanced safeguards for GDPR sensitive PD; Individual data rights; Requirements for downstream data recipients; Redress mechanisms for law enforcement violations

NOW EC US Adeq Dec **adopted & when Cos EU-U.S. Data Priv Framework Certified, then EU SCC not required**

If use SCC, TIA more streamlined due to FISA 702 (but not EO 12333) concerns resolved by EO 14086

CULHANE MEADOWS PLLC

EDPB Opin 2/28 + Info Note on EC US Adeq Dec 7/12

DPRC is significant improvement over prior DoS ombudsperson w/ more effective powers + more safeguards to prevent access to PD re: non-US persons like **DPRC Special Advocates & PCLOB Review BUT concerns re: practical functioning of redress mechanism:**

- **Some DP principles same as former EU-US Privacy Shield (Ex: opt-out consent) EC Final: Opt-in C req'd 4 GDPR Sens PD: health, race & ethnicity, polit/relig/philos beliefs, union memb, sex life.**
- **Lack of specific rules on auto decision making & profiling: EC Final: US Cs subject to GDPR; US Laws prevent: FHA; Civ Rts Act; FCRA; HIPAA.**

- **Concern re: prior independent authorization of surveillance**
  - **None re: EO 12333 re: collection of data in bulk EC Final: Bulk lim'd to 6 Natl Sec objectives: 1 terrorism; 2 hostage taking & holding captives; 3 foreign espionage; 4 sabotage; 5 assassination; 6 WMD.**
- **EO 12333 no independent review by court** or other independent review body
- **DPRC no notice to Data Subjects of violation or determ requiring appropriate remedy**
- **No appeal from DPRC to Court or indep review body outside USG**

CULHANE MEADOWS PLLC

US DOC PS Website Updated for EO 14086 DPF

7/17 US DOC EU/Swiss/UK DPF website live for self-certs

https://www.dataprivacyframework.gov/s/

Cert updates from EU-US **PS to DPF due**:

- **EU 10/10/23**
- **PS/DPF HR & non-HR (marketing) Swiss (due 10/17) + UK too**
- **Updates 1 Yr** Anniv of Cert
- **1st time DPF Applicants**
  - **Implement DPF Principles**
  - **"Publicly declare" commitment to DPF Principles**
  - **Post a DPF compliant website privacy policy** (non-HR; HR internal)
  - **Certify compliance w/ DPF** Principles to US DOC

CULHANE MEADOWS PLLC

FISA 702 Reauth: WH Pres Intell Advisory Bd 13 Recs

7/31/23 FISA 702 Reauth WH Pres Intell Adv Bd Rpt 13 Recs

1. **AG remove FBI auth** to query for **evidence of non-nat'l security crime** in FISA 702 data
2. **DNI & AG estab** rigorous **FISA 702 pre-approval** across USG IC for **U.S. person content** queries
3. **FBI designate FISA 702 CCO** & training across FBI
4. **IC As imp plans for recs 1, 2, & 3 to DNI & AG w/in 2 mos & execute w/in 6 mos**
5. **Senior personnel exchanges to create FBI culture of FISA 702 compliance**
6. **EOP new review mechan to assess FISA 702 compliance** and ensure **corrective action**
7. **DNI & AG research tech to enhance FISA 702 oversight** & rpt to POTUS, C & Intell Oversight Bd
8. **AG prop funding legis** for FISA 702 **oversight**
9. **Declass "to greatest extent possible" FISA 702 categories authorized**
10. **DNI & AG** submit **new FISA 702 counternarcotics cert to FISC**
11. **DNI & AG new stands of accountability** for FISA 702 users
12. **DNI & DOJ prop legis to codify FISA 702 adherence to EO 14086**
13. **DNI & AG prop legis to require amicus curiae in all annual FISA 702 certs to FISC**

Watch this Space for Biden Admin & C action

CULHANE MEADOWS PLLC

US Biden EO 14086 DATA PRIVACY FRAMEWORK: IS IT EU ADEQUATE?

Takeaways

Double – check:

- **GDPR triggers + US FISA Sec 702 & EO 12333 (ECS)**
- **EU-US PD access/transfers/flows compliance**
  - **inc service providers/vendors/biz partners/B2B customers**
  - **Update USG PD request review process & procedures**

Cos certified to EU-US Privacy Shield:

- **Continue PS comply & update website (& HR) privacy policies for EU/Swiss/UK** Non-HR & HR **DPF**
- **Update Data Processing Agmts relying on EU-US PS to DPF**
- **Keep EU & UK SCC in place pending Schrems III**

In Alt: If use EU SCC: make sure using "new" (under GDPR 6/4/21**) ones + update TIAs + Supp Sec Meas** to reflect EU-US DPF Adeq Decision

If trigger GDPR w/o using EU-US PS/DPF or EU/UK SCC: choose 1 (or both (in alternative) **& implement.**

Watch this space for FISA 702 Reauth & Schrems III

CULHANE MEADOWS PLLC

Thanks for Listening!

Linda V. Priebe, JD, CIPP/E
Partner & Co-Chair,
Government, Regulatory & Compliance Practice Group
Culhane Meadows PLLC
Washington, DC
lpriebe@cm.law

CULHANE MEADOWS PLLC