What the EU-US Data Privacy Framework Means for You

Perspectives from the European Union and the United States

TERRALEX

Disclaimer:

The views expressed during this program do not constitute legal advice, belong solely to the panelists, and do not reflect the views of the Association of Corporate Counsel or the entities for whom the panelists are employed.

The EU-US DATA PRIVACY FRAMEWORK

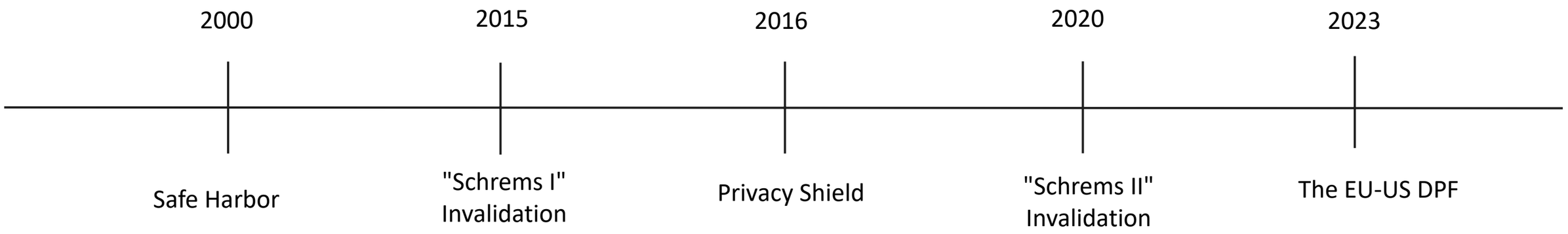
Effective July 10, 2023

Commonly known as the "DPF"

Adequacy Decision under Art. 45 of the EU's General Data Protection Regulation (GDPR) – one of the tools provided under the GDPR to transfer personal data from the EU to third countries that offer a comparable level of protection of personal data to that of the EU

THE HISTORY OF THE DPF

HISTORICAL BACKGROUND



The EU-US DATA PRIVACY FRAMEWORK

EU private and public entities are free to transfer personal data to participating organizations in the US without having to put in place additional data protection safeguards

Equivalent versions apply to transfers from the United Kingdom and Switzerland

THE IMPACT OF THE DPF

Lawful flow of personal data from the European Economic Area (including the 27 EU Member States as well as Norway, Iceland, and Liechtenstein) to US participating organizations that qualify as "controllers" or "processors" as defined in the GDPR

Participation is voluntary for eligible organizations. Organizations that are ineligible or do not wish to self-certify may still use Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other lawful data transfer mechanisms or derogations to obtain personal data from the EU

IS YOUR BUSINESS ELIGIBLE FOR DPF?

Only organizations that are subject to the jurisdiction of 2 federal US agencies may self-certify compliance:

Federal Trade Commission (FTC)

US Department of Transportation (US DOT)

Ineligible organizations include most banks and financial institutions, non-profit organizations, some insurance companies and non-US companies

PROs and CONs OF DPF PARTICIPATION

PROs:

More efficient transfer mechanism - time/cost reduction (for non-US customers)

No need to submit TIAs

Speeds up sales process

Customer trust

PROs and CONs OF DPF PARTICIPATION

CONs:

Resource requirements for participants - implementation costs, fees, audits

Risk of being overturned (Schrems III)

Not a solution for global intra-group data flows - single approach vs. US and rest of the world

UK-US DATA BRIDGE

- Post-Brexit, UK is not covered by the EU-US DPF
- Data Bridge operates as an extension to the EU-US DPF
- Implemented following UK government assessment of the EU-US DPF and of revised US surveillance arrangements
- In effect from 12th October 2023
- Permits data transfers to DPF-certified US organizations
- US recognition of UK as a “qualifying state”, enabling UK individuals access to the redress mechanisms

UK-US DATA TRANSFERS

- Where DPF not used, UK data exporters can continue to rely on UK equivalent of EU SCCs, provided a Transfer Risk Assessment (UK version of the EU's TIA) is also carried out

- UK SCCs are either (i) International Data Transfer Agreement (IDTA) or (ii) Addendum to EU SCCs

THE SELF-CERTIFICATION PROCESS

EU-US DPF is administered by the International Trade Administration (ITA) within the US Department of Commerce

Self-certification can be achieved via Commerce Department's DPF program website:

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

ADHERENCE TO DPF PRINCIPLES

DPF lays out requirements governing participants' use and treatment of personal data, and access and recourse mechanisms that are provided to the EU individuals

US organizations must publicly commit to complying with the DPF principles

Once an organization is certified and commits to adhere to DPF, the commitment is enforceable under US law

MANDATORY ELEMENTS OF COMPLIANCE

DPF-Compliant Privacy Policy

Your policy must comply with DPF principles, both on paper and in practice

Write your policy clearly, concisely and make it easy to understand

Your policy must specifically state that you adhere to the DPF principles, and must include a hyperlink to the DPF website (http://www.dataprivacyframework.gov/)

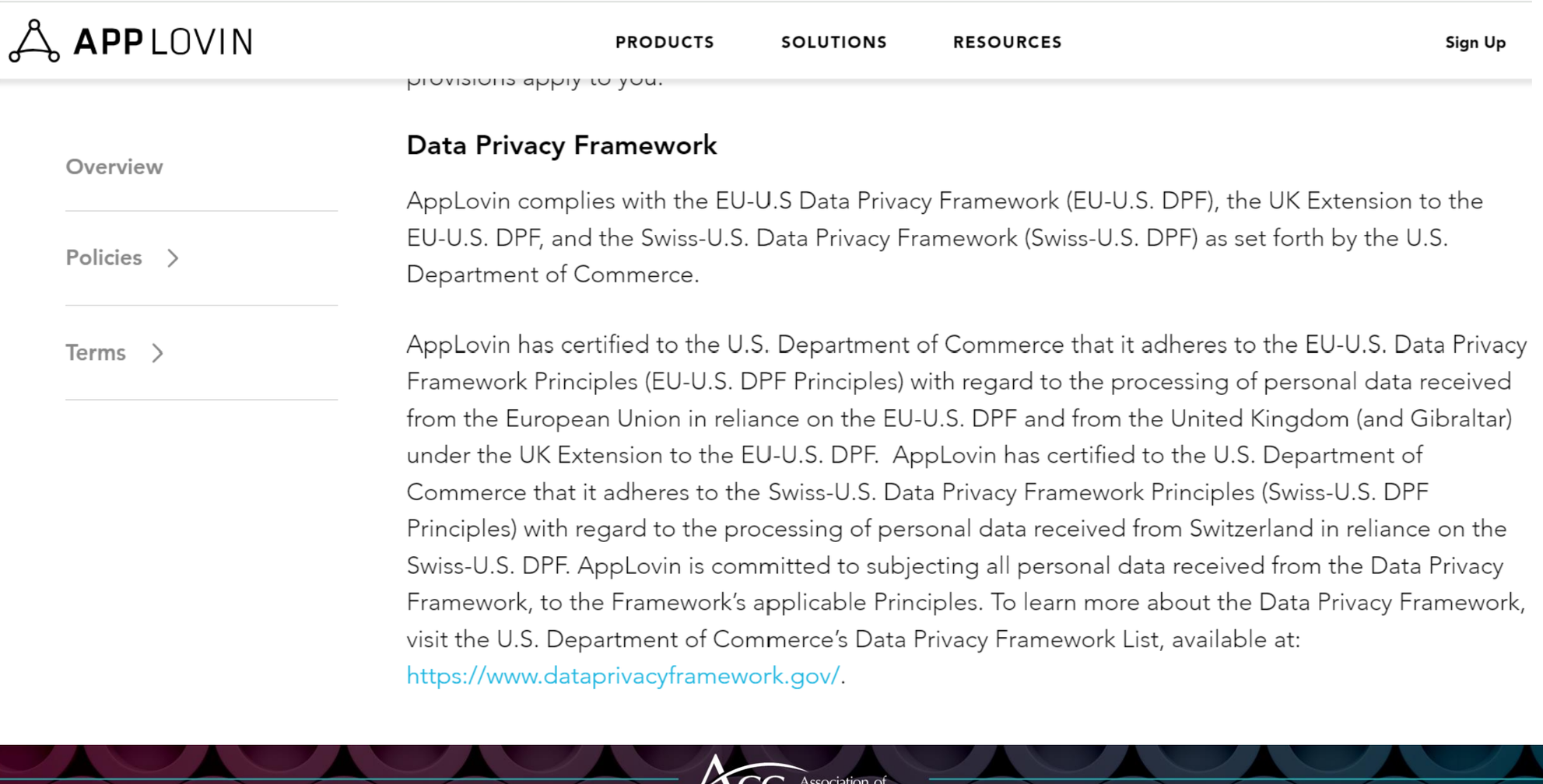
MANDATORY ELEMENTS OF COMPLIANCE

DPF-Compliant Privacy Policy

Your policy must identify your "Independent Recourse Mechanism" clearly

Include a hyperlink to the correct complaint form on the website of the relevant dispute resolution mechanism

DPF-COMPLIANT PRIVACY POLICY



DPF-COMPLIANT PRIVACY POLICY

Overview

Policies >

Terms >

With respect to personal data received or transferred pursuant to the Data Privacy Framework, AppLovin is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, AppLovin may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, AppLovin commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to TRUSTe, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://feedback-form.truste.com/watchdog/request for more information or to file a complaint. These dispute resolution services are provided at no cost to you.

For complaints regarding DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website.

REQUIRED "RECOURSE MECHANISMS"

Organizations must provide recourse for individuals to complain about non-compliance, and lodge complaints for resolution

Effective and readily available recourse mechanisms must investigate and resolve individuals' complaints and disputes **at no cost to the individual**

Organizations may choose independent recourse mechanisms in the European Union or the United States

INDEPENDENT RECOURSE MECHANISMS

KROLL

Data subjects may contact the relevant independent recourse mechanism listed below:

- EU Data Protection Authorities (DPAs)
- Swiss Federal Data Protection and Information Commissioner
- UK Information Commissioner's Office

Kroll will cooperate with the applicable data protection authority in the investigation and resolution of complaints brought under the DPF. Kroll will comply with any advice given by the EU DPAs, the FDPIC, or the ICO where the applicable authority takes the view that the organization needs to take specific action to comply with the DPF Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the applicable authority with written confirmation that such action has been taken.

t what information they collect and how they use the
they outline in their privacy notice. If you have a
your concern and we'll try to help with resolution. We'll

u reside. More information about how to contact your

please click here

THE FINANCIAL COMPONENT OF DPF

The US Department of Commerce maintains a fund supplied with annual contributions by the EU-US DPF organizations that covers the costs of arbitration proceedings before the EU-US DPF Panel

Payment amounts are based on the organizations' annual revenues

THE FINANCIAL COMPONENT OF DPF

Annual Fee Schedule for the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)*:

Organization's Annual Revenue:	A Single Framework / Both Frameworks:
$0 to $5 million	$250 / $375
Over $5 million to $25 million	$650 / $975
Over $25 million to $500 million	$1,000 / $1,500
Over $500 million to $5 billion	$2,500 / $3,750
Over $5 billion	$3,250 / $4,875

*For purposes of the current annual fee schedule described above:

- 'A single framework' could refer to any of the following: only the EU-U.S. DPF; only the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF; or only the Swiss-U.S. DPF
- 'Both frameworks' could refer to any of the following: the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF; or only the EU-U.S. DPF and the Swiss-U.S. DPF.

As organizations that wish to participate in the UK Extension to the EU-U.S. DPF must participate in the EU-U.S. DPF, the annual fee that such organizations are required to pay to the ITA to participate in the EU-U.S. DPF currently covers both the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

THE FINANCIAL COMPONENT OF DPF

- Organizations have additional, direct costs associated with participating in the DPF program. For example, under the relevant part(s) of the DPF program:
- Organizations must provide a readily available independent recourse mechanism to hear individual complaints at no cost to the individual. Private-sector alternative dispute resolution bodies that provide such services with regard to personal data other than human resources data set their own fees. Organizations that are either required or choose to cooperate and comply with the EU DPAs with regard to all data covered by their self-certifications are required to pay an annual fee of U.S. $50 in order to cover the operating costs of the EU DPA panel. This EU DPA panel fee is payable to the United States Council for International Business (USCIB), which has agreed to act as the trusted third party for this purpose (i.e., USCIB serves as the custodian of the funds collected through the EU DPA panel fee, but does not itself serve as an independent recourse mechanism). No such independent recourse mechanism-related fee is required with regard to the UK ICO or the Swiss FDPIC.
- An EU, UK or Swiss individual has the right to invoke binding arbitration to determine whether a participating organization has violated its obligations under the DPF Principles as to that individual and whether any such violation remains fully or partially unremedied. The U.S. Department of Commerce has committed to the maintenance of a fund to which participating organizations are required to contribute to cover the arbitral costs as described in Annex I to the DPF Principles. The International Centre for Dispute Resolution-American Arbitration Association (ICDR-AAA) was selected by the U.S. Department of Commerce to administer arbitrations pursuant to and manage the fund identified in Annex I of the DPF Principles. Information on required contributions is available at https://go.adr.org/dpf-annexi-fund.html.

THE VERIFICATION MECHANISM

Organizations must provide procedures for verifying that the attestations and assertions they make about their EU-US DPF privacy practices are actually true, and that they have actually implemented their privacy practices as they have represented

Self-assessment, outside compliance reviews

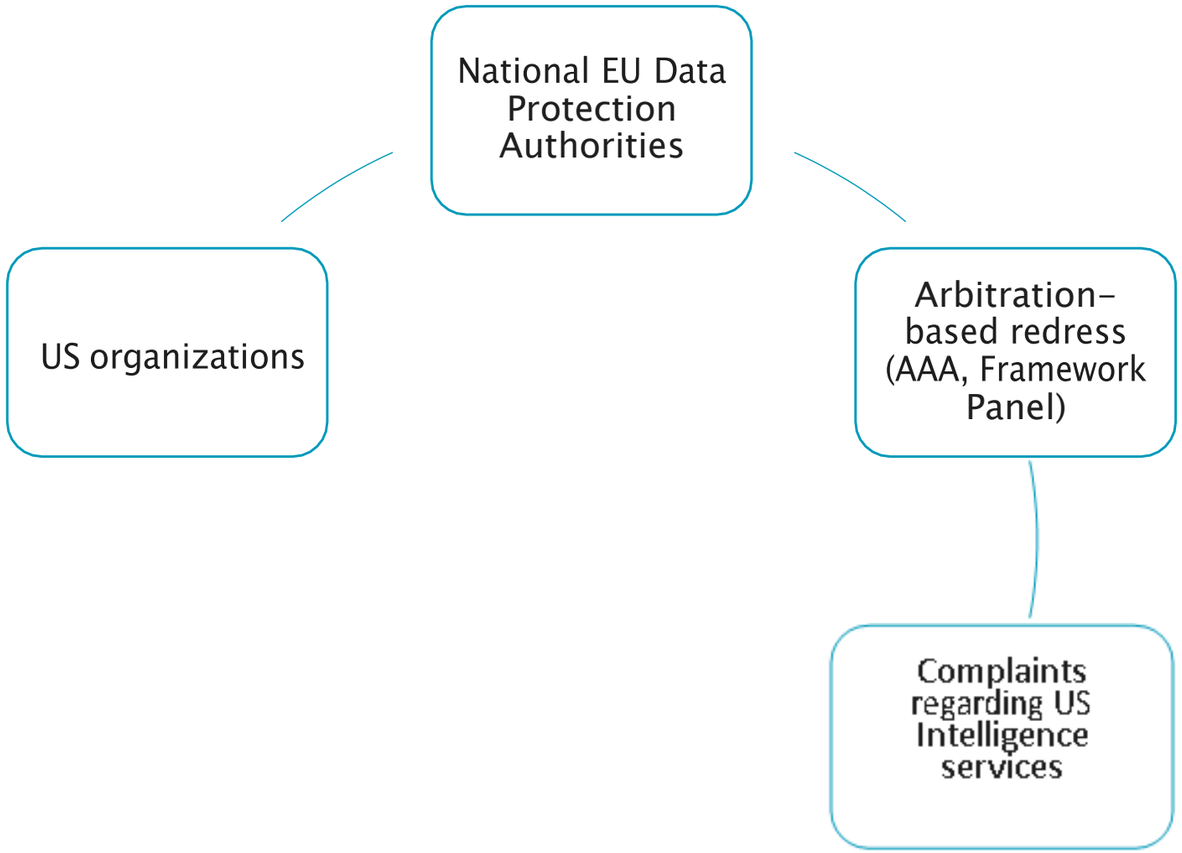
Organizations must identify any third-parties that complete those reviews

PROVIDE A DPF CONTACT

Organizations must identify a contact within their organization to handle complaints, access requests, and any other issues that may arise under the Principles:

- Name
- Job Title
- E-mail address
- Telephone number(s)
- US mailing address

REDRESS MECHANISMS



- EU Data Protection Authorities
- Civil Liberties Protection Officers
- Data Protection Review Court

"ONWARD" TRANSFERS

EU-US DPF expressly prohibits "onward transfers"

Few exceptions:

For limited and specified purposes

For contractual reasons between a DPF organization and a third-party

Only if the contract requires the third party to guarantee same level of protection as that guaranteed by DPF Principles

HOW WILL DPF BE ENFORCED IN THE US?

FTC has indicated its intent to aggressively enforce the DPF in three key areas:

- Referral prioritization and investigations
- Seeking and monitoring orders
- Enforcing cooperation with EU Data Protection Authorities (DPAs)

HOW WILL DPF BE ENFORCED IN THE US?

UNITED STATES OF AMERICA
Federal Trade Commissio
WASHINGTON, D.C. 20580

Office of the Chair

Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

The United States Federal Trade Commission ("FTC" address its enforcement role in connection with the EU-U.S. DPF") Principles. The FTC has long committed to protecting borders, and we are committed to enforcement of the comme framework. The FTC has performed such a role since the yea EU Safe Harbor Framework, and most recently since 2016, i Privacy Shield Framework.[1] On July 16, 2020, the Court of J ("CJEU") invalidated the European Commission's adequacy Privacy Shield Framework, on the basis of issues other than t FTC enforced. The U.S. and the European Commission have Privacy Framework to address that CJEU ruling.

I write to confirm the FTC's commitment to vigorous Principles. Notably, we affirm our commitment in three key areas: (1) referral prioritization and investigations; (2) seeking and monitoring orders; and (3) enforcement cooperation with EU data protection authorities ("DPAs").

c. FTC Enforcement Activity

The FTC brought cases under both the U.S.-EU Safe Harbor and EU-U.S. Privacy Shield frameworks and continued to enforce the EU-U.S. Privacy Shield even after the CJEU invalidation of the adequacy decision underlying the EU-U.S. Privacy Shield Framework.[8] Several of the FTC's recent complaints have included counts alleging that firms violated EU-U.S. Privacy Shield provisions, including in proceedings against Twitter,[9] CafePress,[10] and Flo.[11] In the enforcement action against Twitter, the FTC secured $150 million from Twitter for its violation of an earlier FTC order with practices affecting more than 140 million customers, including violating EU-U.S. Privacy Shield Principle 5 (Data Integrity and Purpose Limitation). Further, the agency's order requires that Twitter allow users to employ secure multi-factor authentication methods that do not require users to provide their telephone numbers.

THE PAST IS PROLOGUE - PRIOR ACTIONS

UNITED STATES OF AMER
Federal Trade Commis
WASHINGTON, D.C. 2058

Office of the Chair

Didier Reynders
Commissioner for Justice
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Reynders:

The United States Federal Trade Commission ("FT
address its enforcement role in connection with the EU-U.S
DPF") Principles. The FTC has long committed to protecti
borders, and we are committed to enforcement of the comn
framework. The FTC has performed such a role since the y
EU Safe Harbor Framework, and most recently since 2016,
Privacy Shield Framework.[1] On July 16, 2020, the Court o
("CJEU") invalidated the European Commission's adequac
Privacy Shield Framework, on the basis of issues other thar
FTC enforced. The U.S. and the European Commission hav
Privacy Framework to address that CJEU ruling.

I write to confirm the FTC's commitment to vigoro
Principles. Notably, we affirm our commitment in three key areas: (1) referral prioritization and investigations; (2) seeking and monitoring orders; and (3) enforcement cooperation with EU data protection authorities ("DPAs").

In *CafePress*, the FTC alleged that the company failed to secure consumers' sensitive information, covered up a major data breach, and violated EU-U.S. Privacy Shield Principles 2 (Choice), 4 (Security), and 6 (Access). The FTC's order requires the company to replace inadequate authentication measures with multifactor authentication, substantively limit the amount of data it collects and retains, encrypt Social Security numbers, and have a third party assess its information security programs and provide the FTC with a copy that can be publicized.

In *Flo*, the FTC alleged that the fertility-tracking app disclosed user health information to third-party data analytics providers after commitments to keep such information private. The FTC complaint specifically notes the company's interactions with EU consumers and that Flo violated EU-U.S. Privacy Shield Principles 1 (Notice), 2 (Choice), 3 (Accountability for Onward Transfer), and 5 (Data Integrity and Purpose Limitation). Among other things, the agency's order requires Flo to notify affected users about the disclosure of their personal information and to instruct any third party that received users' health information to destroy that data. Importantly, FTC orders protect all consumers worldwide who interact with a U.S. business, not just those consumers who have lodged complaints.

HOW WILL DPF BE ENFORCED IN THE US?

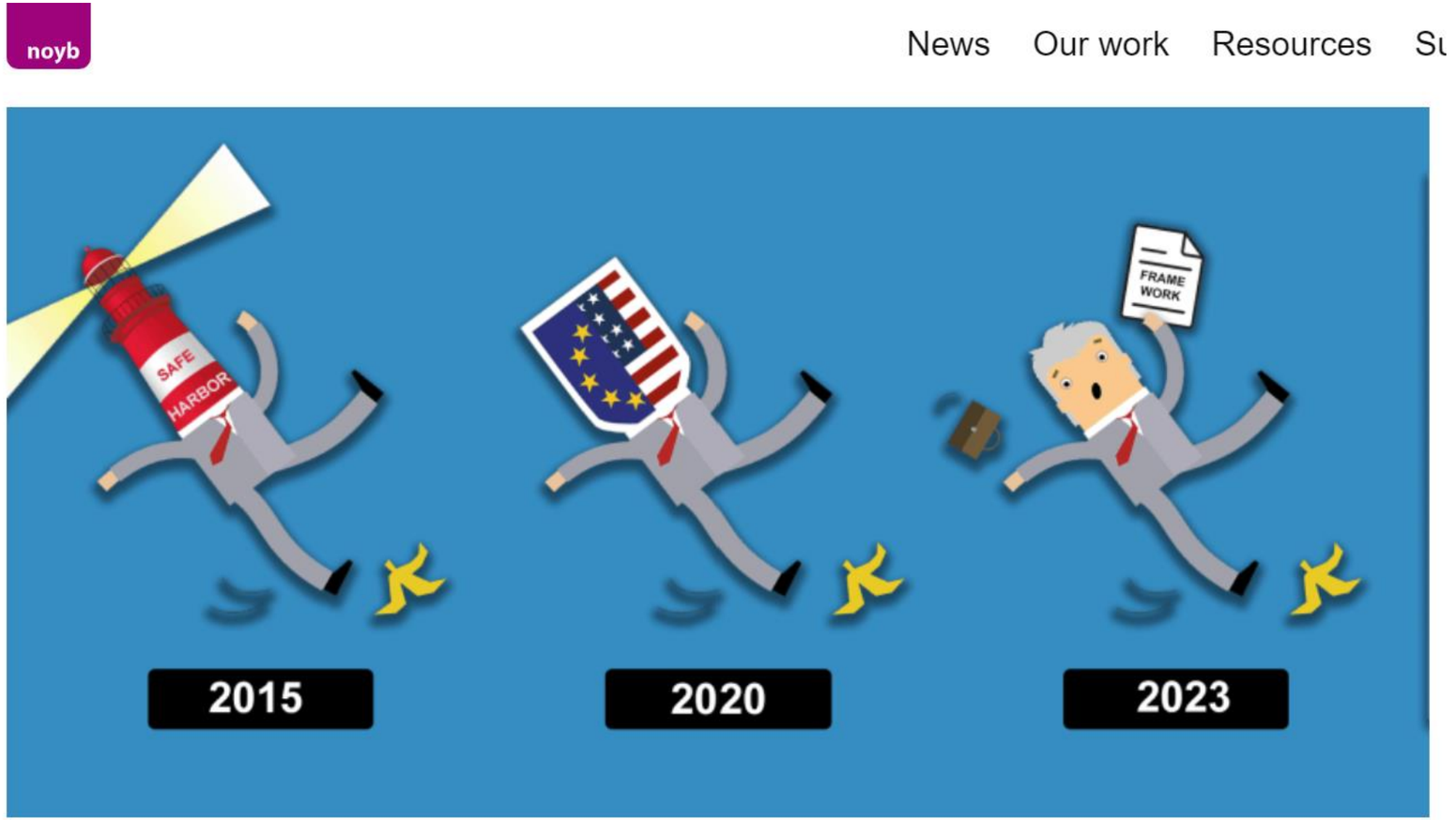
Civil penalties of up to $50,120 per violation, or $50,120 per day for continuing violations

FTC orders against companies will require ongoing reporting to the FTC of redress of violations and strengthened measures for security

SAFE WEB Act - 15 USC 41 et seq.

- Increased cooperation with foreign law enforcement authorities through confidential information sharing and provision of investigative assistance

LOOKING AHEAD - SCHREMS III?



LOOKING AHEAD - SCHREMS III?

Will we see a Schrems III that seeks to invalidate DPF because of US government surveillance?

On his website, None of Your Business (NYOB), Mr. Schrems has already argued that DPF is fundamentally flawed because the US affords constitutional rights only to US citizens, and EU data is still subject to mass surveillance

ALTERNATIVES TO DPF

Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other lawful data transfer mechanisms when transferring personal data to US organizations that are not certified for the EU-US DPF

Transfer Impact Assessments (TIAs) for transfers to organizations that are not certified

UK-US DATA TRANSFERS: PRACTICAL POINTS

- December 2023: indirect benefit of DPF = guidance from ICO simplifying TRAs for US transfers. UK organizations can refer to DSIT's DPF assessment using template wording

- 21 March 2024: deadline for updating legacy contracts (pre-21 September 2022) containing old SCCs

Thank You!/Questions/Contact Info

- Kelly R. Melchiondo, *Bilzin Sumberg (Miami, Florida)*
  - *kmelchiondo@bilzin.com*
- Joelle G. Dvir, *AppLovin' (Miami, Florida)*
  - *Joelle.dvir@applovin.com*
- Violetta Kunze, *Djingov, Gouginski, Kyutchukov & Velichkov (Sofia, Bulgaria)*
  - *Violetta.Kunze@dgkv.com*
- Jon Bartley, *RPC (London, United Kingdom)*
  - *Jon.Bartley@rpc.co.uk*