SQUIRE PATTON BOGGS

Crossing The Atlantic: Top Tips for Completing Your Data Privacy Framework Certification

September 14, 2023

Who We Are

SQUIRE PATTON BOGGS

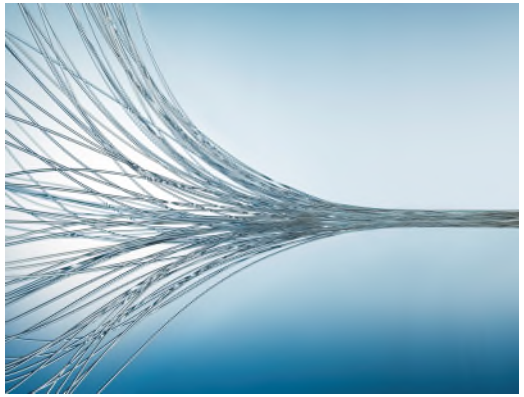
Charles Helleputte
Partner, Brussels
Charles.Helleputte@squirepb.com

Malcolm Dowden
Co-head of Knowledge Management, London
Malcolm.Dowden@squirepb.com

Julia Jacobson
Partner, New York
Julia.Jacobson@squirepb.com

What We'll Cover

SQUIRE PATTON BOGGS

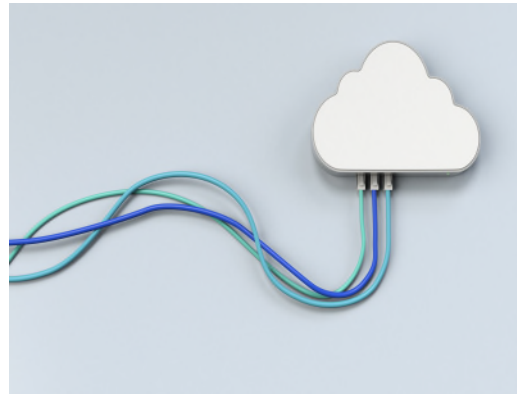


Data Privacy Framework: The Origin Story

DPF Basics

DPF Certification Tips and Traps

Should We / Shouldn't We Certify



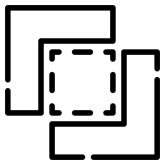
SQUIRE PATTON BOGGS

The DPF Origin Story

The Transfer Playbook

ADEQUACY

SAFEGUARDS



DEROGATIONS

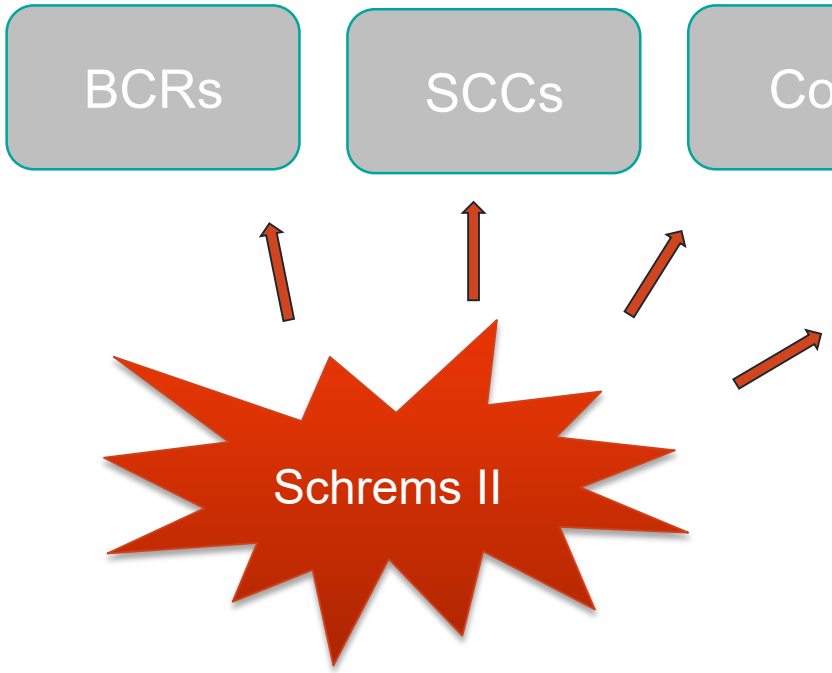
Art. 46.1 GDPR:

'a controller or a processor may transfer personal data to a third country […] only if the controller or processor has provided appropriate safeguards, and on conditions that enforceable data subject rights and effective legal remedies for data subjects are available.'

- BCRs (binding corporate rules)
- SCCs (standard contractual clauses)
- Codes of Conduct
- Certification

Schrems II?

- Judgment by the Court of Justice of the EU
- Invalidated EU/US Privacy Shield
- And had a much broader impact



- *Schrems II* affects <u>all</u> personal data transfers to a non-EEA / adequate country subject to 'appropriate safeguards'
- Challenges with derogations in Art. 49 GDPR

The New DPF

- 25 March 2022, the EU Commission and the US agreed in principle on a new Trans-Atlantic Data Privacy Framework for personal data transfers
- 7 October 2022, US President Joe Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities

  - ✓ Safeguards limiting data collection by intelligence agencies to what is necessary and proportionate
  - ✓ Oversight procedures within intelligence agencies
  - ✓ New multi-stage redress mechanism to address individuals' complaints

10 July 2023: EU adopted its adequacy decision

Next: 'To Do' for companies and organizations:

- Adhere to the Principles
- Self-certify through the US Department of Commerce
- Watch developments of DPF challenges (*Schrems III*)

The UK Extension?

SQUIRE PATTON BOGGS

- DPF is an EU adequacy decision. UK GDPR is (post-Brexit) a separate law.
- Effective as of July 17, 2023 eligible organizations in the United States that wish to self-certify their compliance pursuant to the UK Extension to the EU-U.S. DPF may do so; however, personal data cannot be received from the United Kingdom and Gibraltar in reliance on the UK Extension to the EU-U.S. DPF before the date that the adequacy regulations implementing the data bridge for the UK Extension to the EU-U.S. DPF enter into force.
- UK adequacy regulations are made under Data Protection Act 2018, s 17A.
- No fixed date yet for UK regulations. Parliament is in recess until 16 October. Possible – but not certain – that UK regulations will be in place by the end of 2023.

Switzerland?

SQUIRE PATTON BOGGS

- DPF is an EU adequacy decision. Switzerland is not an EU or an EEA member state.
- The effective date of the Swiss-U.S. DPF Principles, Supplemental Principles and Annex I of the Principles is July 17, 2023; however, personal data cannot be received from Switzerland in reliance on the Swiss-U.S. DPF until the date of entry into force of Switzerland's recognition of adequacy (i.e., entry into force of the expected recognition by the Swiss Federal Administration that the Swiss-U.S. DPF ensures data protection consistent with Swiss law).
- At present the US does not appear on the list of adequate countries contained in Annex I of the new Swiss Federal Data Protection Act but the list is expected to be amended in due course.

SQUIRE PATTON BOGGS

DPF Basics

Eligibility

SQUIRE PATTON BOGGS

U.S. legal entities that are subject to the investigatory and enforcement powers of:

(1) Federal Trade Commission (***FTC***) – The FTC Act grants the FTC authority over acts or practices affecting interstate commerce by any person, partnership or corporation. Generally, this means **businesses operating for profit in the U.S**.; and/or
(2) Department of Transportation (***DOT***) - The DOT has authority to enforce the privacy practices of **U.S. and foreign air carriers serving the U.S., as well as the ticket agents that market air transportation**.

The DOT and the FTC share jurisdiction over ticket agents that market air transportation.

Also:

- Covered entities and business associates operating *for-profit* under the federal Health Insurance Portability and Accountability Act of 1996
- Most U.S. trade and professional associations
- Entities regulated by the Federal Communications Commission (FCC) if they also are subject to FTC jurisdiction

DPF Website

SQUIRE PATTON BOGGS

- International Trade Administration (ITA) of Department of Commerce (DoC) maintains the DPF Website and DPF List, processes applications, re-certifications, removals from DPF List, etc.
  - DPF Website: www.dataprivacyframework.gov
  - DPF List: https://www.dataprivacyframework.gov/s/participant-search
  - DoC's FAQs: https://www.dataprivacyframework.gov/s/article/FAQs-dpf

- A U.S. business with an "**Active**" Privacy Shield Certification is automatically part of DPF - ***as long as*** the business' privacy policies and procedures are updated to reflect the DPF Principles by (i) October 10, 2023 for the EEA and UK/Gibraltar and (ii) October 17, 2023 for the Swiss DPF.
- A business listed as "**Inactive**" on the DPF List – whether because the business withdrew from Privacy Shield or did not complete the annual re-certification – can use its DoC account to complete the DPF certification process but must re-apply (…although the DoC's FAQs are not completely clear on this point …)

Covered Data

SQUIRE PATTON BOGGS

- **HR Data** - personal data about past and present employees collected in the context of the employment relationship
  - personal data collected from applicants and independent contractors presumably is covered as non-HR Data.

- **Non-HR Data / Customer Data** - personal data collected from or about a customer, client, website visitor app user

- *Partial* exemptions for
  - “public record information”
  - “personal data from publicly available sources”

DPF Principles

SQUIRE PATTON BOGGS

Seven Core Principles

1. **Notice**: The Notice Principle requires a certified business to inform EU citizens about their rights and the DPF certified business' obligations under DPF. The certified business must provide the notice at the time of collection or "as soon thereafter as is practicable". Supplemental Principle 9 includes additional obligations for HR Data.

2. **Choice**: DPF requires a certified business to offer certain choices to individuals whose personal data is received by the business under DPF. These choices are the opportunity to **opt out** of:
   - the disclosure of their personal data to another ***Controller*** (i.e., an organization that, alone or jointly with others, determines the purposes and means of the processing of personal data);
   - the use of their personal data for a purpose that is materially different from the purpose(s) for which the personal data was originally collected (as described in the relevant notice) or subsequently authorized by the individual; and
   - having personal data used for direct marketing. This direct marketing opt-out right is "subject to reasonable limits" established by the certified business, such as "time to make the opt out effective" (see Supplemental Principle 12).

   Choice also requires "affirmative express consent" before disclosing sensitive information to a third party or before using the sensitive information for a purpose not covered in the original notice or authorized by the affirmative express consent.

DPF Principles

SQUIRE PATTON BOGGS

Seven Core Principles, *cont.*

3. **Accountability for Onward Transfers**: DPF requires a certified business to comply with certain procedures and impose certain contractual terms when transferring personal data received from the EU (and UK and/or Switzerland). [*More on this later*]

4. **Security:** DPF requires that a certified business take reasonable and appropriate measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. **Data Integrity and Purpose Limitation**: DPF generally requires a certified business (i) to use and retain personal data only for the purposes for which it has been collected or subsequently authorized by the individual and (ii) to take reasonable steps to ensure the reliability of personal data for its intended use.

DPF Principles

SQUIRE PATTON BOGGS

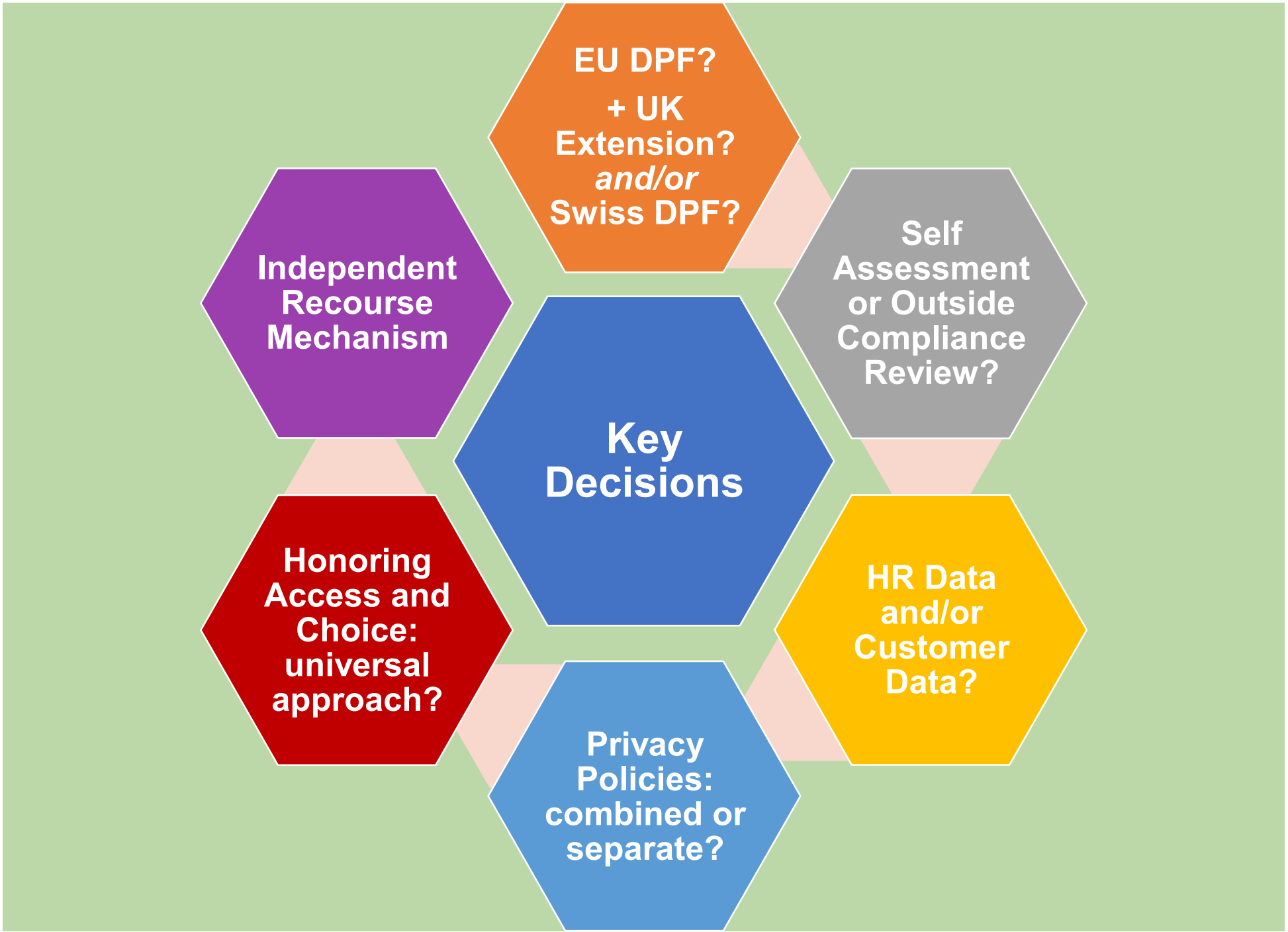
Seven Core Principles, *cont.*

6. **Access**: DPF requires a certified business to allow individuals to access their personal data. Subject to some exceptions and exemptions, a certified business must allow individuals to correct, amend, or delete inaccurate personal information or personal information processed in violation of DPF.

   Supplemental Principle 8 includes details on how to operationalize the Access Principle, such as when a business can deny or limit access and when a business may charge a fee for providing access. Supplemental Principle 9 explains that, for HR Data, the certified business is expected to cooperate with EU employers.

7. **Recourse, Enforcement, and Liability**: DPF requires a certified business to implement robust recourse mechanisms, cooperate with authorities, and arbitrate claims in accordance with DPF. Additional requirements apply for HR Data. Supplemental Principle 11 sets out additional details for Dispute Resolution and Enforcement

Getting Started



SQUIRE PATTON BOGGS

DPF Certification Tips and Traps

Tips and Traps

SQUIRE PATTON BOGGS

DPF Privacy Policy/ies

- For non-HR Data
  - Must be public
- For HR Data
  - Can be public *or* private
- Combined privacy policy for HR and non-HR Data
  - Must be public
- Combined into non-DPF Privacy Policy
  - Must be public

Tips and Traps

The DPF Website provides sample provisions for explaining:

- certification to the two Frameworks and UK Extension
- FTC and/or DoT authority
- internal complaint process

Also need internal policies and procedures for choice, access, tracking opt-in/opt-out consent and affirmative consent for sensitive information, recordkeeping, and verification.

Tips and Traps

SQUIRE PATTON BOGGS

Handling Choice and Access

- global vs. local approach
- depending on how the certified businesses currently handles U.S. privacy rights, GDPR data subject rights or privacy rights under other applicable laws, DPF may require some changes or additions to current processes, technology, staffing.

Tips and Traps

SQUIRE PATTON BOGGS

Onward Transfers and Privacy Contracts

- See Supplemental Principle 'Obligatory contracts for Onward Transfers' (Annex I, Section III.10.b).
  - While this Principle allows for transfers based also on non-contractual instruments (e.g., intra-group compliance and control programs), the text makes clear that these instruments must always "ensur[e] the **continuity of protection** of personal information **under the Principles**".

Tips and Traps

SQUIRE PATTON BOGGS

Onward Transfers and Privacy Contracts: Annex I.II 3b (transfer to agent/processor)

- To transfer personal data to a third party acting as an “agent” , a certified business must: (i) transfer personal data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization’s obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

Tips and Traps

SQUIRE PATTON BOGGS

Onward Transfers and Privacy Contracts: Annex I.II 3a (transfer to controller)

- To transfer personal data to a third party acting as a controller, a certified business must comply with the Notice and Choice Principles. The certified business also must "enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate."

Tips and Traps

SQUIRE PATTON BOGGS

Choosing an independent recourse mechanism (IRM)

- An IRM is intended to ensure compliance with the DPF by allowing EU individuals (and/or UK and/or Swiss individuals, as applicable) to submit complaints to an independent third party that can investigate and resolve the individual's complaints at no cost to that individual.
- The IRM can award monetary damages, injunctive relief and impose sanctions, which "should include publicity for findings of non-compliance and the requirement to delete data in certain circumstances" (Supplemental Principle 11.e)
- For *HR Data*, the business must commit to cooperate with the EU data protection authorities (***EU DPAs***) under the EU-U.S. DPF; the UK Information Commissioner's Office (***ICO***) and, as applicable the Gibraltar Regulatory Authority (***GRA***) under the UK Extension to the EU-U.S. DPF; or the Swiss FDPIC under the Swiss DPF.
- For *non-HR Data*, several private-sector options are available.

Tips and Traps

Should the Standard Contractual Clauses stay?

- Hedging that the DPF will survive Schrems III

Middle Ground?

Should the Standard Contractual Clauses go?

- Eliminate 'double liability' - DPF and contractual liability

SQUIRE PATTON BOGGS

To Certify or not Certify, that is the Question.

Should We / Shouldn't We

We Should

a) No SCCs means more flexibility in contracting (SCCs must be used verbatim)
b) No TIAs
c) a) + b) = cost savings
d) No data exporter needed

We Shouldn't

Past predicts future and DPF goes the way of its predecessors.

Questions

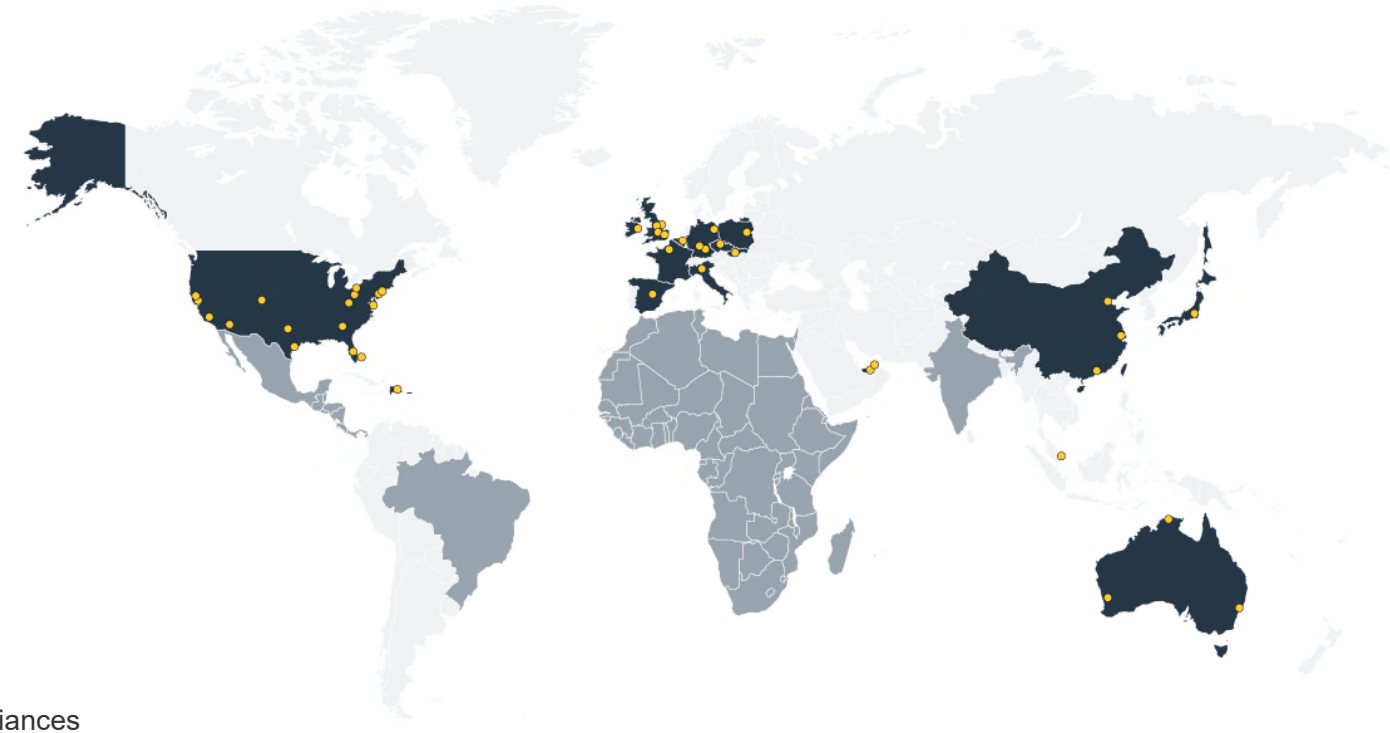
Visit PrivacyWorld.blog for more DPF content.

SQUIRE PATTON BOGGS

Global Coverage

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Dubai
Dublin
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Milan
New Jersey
New York
Palo Alto
Paris
Perth
Phoenix
Prague
San Francisco
Santo Domingo
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico



Office locations

Regional desks and strategic alliances