ABSTRACT

Can EU cross-border data transfer restrictions be eliminated at the State level?

EU cross-border personal data transfer restrictions are designed to ensure that the level of protection of personal data guaranteed under the Treaty of Lisbon and the General Data Protection Regulation (GDPR) is not undermined by exporting data. A heavy compliance burden is currently imposed on US entities that import EU personal data because the US regulatory data protection framework differs from the EU framework in ways that, from an EU perspective, undermine the effective protection of EU data if exported. Lack of compliance with these burdensome obligations can result on administrative fines of 20,000,000 Euros or in case of an undertaking, 4% of the total worldwide annual turnover of the preceding financial year (GDPR Article 83.5(c)). That compliance burden not exist for entities exporting data into a territory that is deemed adequate from EU perspective. This paper intends to answer the question of whether data protection could be regulated at the State level in a way that would reduce or eliminate EU cross-border compliance burden while not violating US constitutional limitations on the regulatory powers of US States.

Under GDPR, international personal data transfers are prohibited unless (a) the entities exporting the data comply with a strict number of requirements that offer sufficient protection (appropriate safeguards), (b) the specific transfer falls within one of seven narrowly defined exceptions (derogations), or (c) the data is exported into a jurisdiction that offers a level of protection deemed adequate (adequacy).

There are several mechanisms US entities can rely on to ensure appropriate safeguards but they are either cumbersome (i.e. the use of non-negotiable contractual clauses pre-approved by Supervisory Authorities) or require a heavy investment not viable for middle and small size companies (i.e. Binding Corporate Rules).

Derogations are exceptional situations narrowly defined under GDPR Article 49. Any entity that decides to rely upon them as a standard method to export EU data will likely face a hefty fine.

Adequacy is the most efficient method to ensure compliance with EU cross-border transfer rules. Although US cannot secure a finding of adequacy based on the existing federal regulatory data protection framework, the US Department of Commerce has requested and obtained a finding of adequacy for a voluntary compliance program known as Privacy Shield. Privy Shield was deemed “adequate” by the European Commission on July 12, 2016[1]. Over 2,700 US organizations rely on Privacy Shield to

[1] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

transfer EU data[2]. However, Privacy Shield is not an optimal adequacy framework for three reasons:

- Privacy Shield is not available to all US entities: Privacy Shield is only available to organizations that are not under the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT).
- Privacy Shield imposes significant obligations: US-based organizations have to apply to join the Privacy Shield and re-certify annually, pay a fee, introduce specific modifications to the privacy notices, and identify and pay for an independent verification mechanism and an independent dispute resolution mechanism.
- Privacy Shield is far from safe: It's predecessor (Safe Harbor) was brought down September 23, 2015 by a decision from the European Court of Justice[3]. Privacy Shield could meet the same fate in the near future[4].

Under GDPR a territory can request and obtain an adequacy determination. The questions that this paper will answer are (1) whether a US State could apply for and obtain an adequacy determination that is far more efficient than Privacy Shield and (2) whether a State privacy framework that qualifies for adequacy under GDPR Article 45 would be viable given the limitations imposed on State regulatory powers by the US constitution and existing federal data protection laws.

[2] https://www.privacyshield.gov/list

[3] Schrems v. Data Protection Commissioner http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=133767

[4]Article 29 Working Party (a working group that includes all EU data protection authorities) has already raised concerns in respect to both the commercial and national security aspects of the Privacy Shield framework and stated that, if those concerns are not addressed within specified timeframes, it may bring legal action to challenge the Privacy Shield's validity. See Article 29 WP Opinion on Privacy Shield https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/12/WP-29-Privacy-Shield-Opinion.pdf (update link to EC website instead)

OUTLINE

Contents

DETAILED OUTLINE

Requirements for EU Cross-border data transfers

- Under GDPR, any transfer of personal data to third countries or international organizations which are undergoing processing or are intended for processing after transfer is prohibited unless the conditions laid out in Chapter V of GDPR are met.
    - Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place ONLY IF the provisions of GDPR are compiled by controller and processor (including onward transfer requirements) GDPR Article 44
- There are three exceptions to the general rule of prohibition[5]:
    - On the basis of adequacy (GDPR Article 45)
    - Subject to appropriate safeguards (GDPR Article 46) including:
        - Binding corporate rules (GDPR Article 47)
    - On the basis of seven specific narrowly interpreted exceptions called "derogations" (GDPR Article 49)
- An adequacy determination is a decision by the European Commission that a specific country, territory, specific sector within a country or an international organization ensures a level of protection for the EU data transfer that is adequate.
    - A transfer of personal data to a third country or international organization may take place where the European Commission has decided that the third country, territory or one or more specific sectors within that third country, or international organization in question ensures an adequate level of protection.
    - Under GDPR, the European Commission may decide that a "third country, a territory or one or more specific sectors within that third country", or a "international organization" ensure an adequate level of protection.
    - As of this date, the European Commission has found adequate the following countries, territories and sectors: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guersey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the US Privacy Shield framework[i].

[5] https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/rules-international-transfers-personal-data_en

    - Except for the Privacy Shield adequacy decision (and that of its predecessor, Safe Harbor), all of the adequacy decision adopted so far relate to countries or to territories of EU countries.
- Infringement of cross-border data transfer requirements are subject to administrative fines of up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (whichever is bigger). (GDPR Article 83.5 (c))

Adequacy

- Adequacy decisions adopted by European Commission[6][7]
    - Andorra
    - Argentina
    - Canada (commercial organizations)
    - Faroe Islands
    - Guernsey
    - Israel
    - Isle of Man
    - Jersey
    - New Zealand
    - Switzerland
    - Uruguay
    - 2016 EU-US Privacy Shield
- All 12 decisions currently under review[8]:
- Adequacy decisions do not cover:
    - Data exchanges in the law enforcement sector which are governed by the "Police Directive" (article 36 of Directive (EU) 2016/680[9]
- Reviewability:
    - If, after assessing the factors laid out above, the European Commission assessment is favorable, the decision will be reflected in an implementing act that will shall provide for a mechanism of periodic review, at least every four years, which shall take into consideration all the relevant developments.

---

[6] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
[7] http://europa.eu/rapid/press-release_IP-16-433_en.htm
[8] https://www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/

https://uk.practicallaw.thomsonreuters.com/w-004-0500?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1
[9] Special arrangements concerning exchanges of data in this field, include PNR (Passenger Name Record) and TFTP (Terrorist Financing Tracking Programme) agreements

    - The European Commission shall monitor the developments that could affect the adequacy decisions adopted. Where the conditions required for adequacy are no longer meet, the European Commission shall, to the extent necessary, repeal, amend or suspend the adequacy decision.
- Adequacy and specifically, “Privacy Shield”, is the most common method used by US organizations importing EU data into the US.
    - Over 2700 US organizations are Privacy Shield certified.

Advantages of exporting EU data under adequacy

- A transfer on the basis of adequacy is basically treated under GDPR as a non-export:
    - Does not require any specific authorization by EU data protection authorities,
    - Does not require adhering to cumbersome non-negotiable contractual clauses with the entity exporting the data,
    - Except for Privacy Shield, entities exporting under adequacy do not need to apply or obtain any special certification before exporting.
    - Except for Privacy Shield no adequacy finding has been challenged in court.

Suboptimal adequacy under “Privacy Shield”

- Currently, the only US entities able to export under adequacy are those that certify under Privacy Shield.
- “Privacy Shield” is suboptimal adequacy:
    - It is available only to entities under the jurisdiction of the FTC
    - It requires the filing of a long application before the department of commerce and an annual re-certification process
    - It faces uncertainty as it could be challenged before EU courts and meet the same fate as its predecessor (Safe Harbor)

Optimal adequacy under State Adequacy:

- GDPR allows for a US State to apply for and obtain adequacy
    - A US State qualifies as a “territory” under GDPR
- State adequacy is optimal adequacy:
    - It will automatically apply to all entities that reside in such State
    - It will not require any fillings
    - Although it could be challenged before EU courts, mechanism could be put in place at the State level to ensure it survives such challenges
- OPTIONS for State adequacy:
    - State level “Privacy Shield” program.
        - Theoretically possible but would provide low value as it does not solve the suboptimal aspects of Privacy Shield.
    - State level comprehensive data protection laws

        - Adequacy based on regulatory approach at the State level that meets the adequacy EU standards.
    - CONCLUSION: Acknowledge the existence of this possibility but state that this paper will look into option two (adoption of data protection laws at the State level)

Qualifying for Adequacy:

What level of data protection regulation would be required to obtain an adequacy decision:

Elements taken into consideration when assessing adequacy

- When assessing adequacy level of protection, the European Commission:
    - Will take into account:
        - Rule of law
        - Respect for human rights and fundamental freedoms
        - Relevant legislation, both general and sectoral including concerning public security, defense, national security and criminal law and the access of public authorities to personal data; and implementation of such legislation;
            - Reference: Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner
        - Data protection rules;
        - Professional rules and security measures, including rules fo the onward transfer of personal data to another third country or international organization with are complied with in that country or international organization
        - Case-law
        - Effective and enforceable data subject rights
        - Effective administrative and judicial redress for the data subjects whose personal data are being transferred.
    - The existence and effective functioning of one or more independent supervisory authorities with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of EU Member States.
    - The international commitments or other obligations arising from legally binding conventions or instruments as well as from participation in multilateral or regional systems, in particular in relation to the protection of personal data.

What is the minimum-viable approach to comprehensive data protection viable in terms of obtaining adequacy?

Research

- NOTE: Privacy Shield has been considered adequate despite the fact that is (1) limited to EU data (2) Principle based with limited actual regulatory requirements. However, all countries that have received an adequacy finding so far are comprehensive data protection countries.
- Research: Japan is currently seeking adequacy but is not a comprehensive data protection country. Developments on that process could provide insights that are valuable for this paper.
- QUESTION: Would a State level law adopting a principle based approach to data protection in the lines of Privacy Shield suffice to consider the State adequate?

Would a comprehensive data protection framework at the State level be constitutional?

General principles: Relevant Constitutional limitations to State regulatory powers

State regulation of interstate commerce: Dormant commerce clause

- There is no grant of power to States to regulate intrastate commerce. However, State regulation that affects intrastate commerce is tolerated in certain cases under police power (health, safety, welfare, morals, aesthetics).
    - To the extent that data protection regulations can be strongly connected to police power, State regulatory powers are strengthen.
- Limitations to State power to regulate interstate commerce:
    - Pre-emption and supremacy clause
    - Vagueness and over breath
    - Contract clause
    - Equal protection
    - Due process
    - Privileges and immunities (if affecting individuals but not for corps)
- Any regulation at the State level is a burden on interstate commerce that must be justifiable under the corresponding test (Rational basis if non discriminatory / Intermediate standard if discriminatory)
- NOTE: Market participant exception: The commerce clause does not prevent a State from preferring its own citizens when the State itself is buying/selling products or hiring labor (White v. Massachusetts) OR giving subsidiaries (Hughes v. Alexandria Scrap Corp.)

Freedom of Expression

- RESEARCH:
    - How does Freedom of Expression limit the ability of States to regulate data protection?
    - Are those limitations different from the limitations that would apply at the Federal level?

- Would those limitations have an impact on the State ability to enact a regulatory framework that would be considered “adequate” from a EU perspective?

Other

- Research:
  - Are there other Constitutional limitations to the State ability to regulations that would enable the State to become “adequate”?

Conclusion

-

Would State enacted data protection law that qualifies for “adequacy” be constitutionally pre-empted by existing Federal level data protection regulations?

Federal regulation of interstate commerce clause:

- Limitations of Fed Gov. ability to regulate the intrastate commerce (Source of Fed power = Commerce power –very broad)
  - FIRST LIMITATION: US Constitution 10th Amendment STATE SOVERGNITY: Any power not grated to the Federal Government belongs to the State or to the People
    - Fed. Gov. can’t commandeering States/State officials:
      - STATE: NY v. US: Federal government cannot commandeer states into action to effectuate federal policy if Congress had no authority in the first place.
      - STATE OFFICIAL: Congress prohibited from commandeering state officials by requiring states to regulate their own citizens. (Printz v. US striking portions of a federal gun law that required state law enforcement officers to collect reports from gun dealers re. prospective owners and conduct background checks).
    - BUT Fed. Gov. can regulate States by prohibiting them from performing certain acts. (Reno v. Condon upholding federal act that bars states and private resellers from disclosing personal information required on drivers’ licenses applications)
  - SECOND LIMITATION: Vagueness or over breath
  - THIRD LIMITATION: Other Con Law limitations such as due process
- Federal commerce power is very broad
  - Affectation Doctrine: To be within Congress’s powers under the commerce clause, a federal law must either
    - Regulate the channels of interstate commerce
    - Regulate the instrumentalities of interstate commerce and persons and things in interstate commerce, or

        - Regulate activities that have a substantial effect on interstate commerce
    - Cumulative impact doctrine (aka National economic impact of intrastate activity)
        - Federal government can regulate intrastate activity because the activity affects other states (e.g. fed law mandating removal of all lead paint from all private and public buildings) OR has an effect on the national economy (Wilckar v. Filburn: Production of wheat for home consumption affect supply/demand of market).
          US. v. Lopez: Source of power 1995: Limits congressional power to regulate local activities (wholly intrastate activities). Court no longer allows testimony regarding Congressional intent when government asserts national economic impact justification for regulation of wholly intrastate activities. Congressional intent must appear either on the face of the law or in the legislative history
            - Non commercial economic activity (Intermediate Scrutiny text – Substantially related to an important State interest): Court likely to strike down the law (particularly if the activity has historically been regulated by local law) Fed. Gov must prove with legislative history (US v. Lopez: federal statute barring possession of gun in school invalid / US v. Morrison: federal civil remedy for victims of gender-motivated violence is invalid)
            - Economic or commercial activity (Rational basis scrutiny test: Reasonably related to a legitimate State interest): If a court can conceive rational basis under which Congress could conclude the activity in aggregate substantially affects interstate commerce the regulation is valid (Gonzalez v. Raich: upholding regulation of intrastate marihuana cultivation –permitted by sate for medical purposes- because it was part of comprehensive fed program to combat interstate traffic in illicit drugs.
        - Administrative convenience (aka Enterprise theory): Intrastate activity may be regulated for (a) administrative convenience OR (b) to avoid piecemeal regulation because there is need for a national/industrial uniform regulation. Hypo: Fed gov already regulates part of an enterprise/industry sector and should be able to regulate entire enterprise/industry sector (including intrastate part). E.g. national health crisis cause by epidemic can't rely on piecemeal legislation. Heart of Atlanta: Law against discrimination in hotels in south against blacks valid under enterprise theory because it impedes travel and can't have piecemeal regulation of the industry.

Existing Federal Data Protection regulations and their approach to pre-emption of State level regulation on the field they regulate

- Research: Current fed level data protection statutes and their stand of pre-emption of State level regulations:
    - GLBA: Does not pre-empt State regulation
        - Find court decision finding Cal-FIPPA is not pre-empted by GLBA bc GLBA only sets a minimum bar
    - FCRA: Does pre-empt State regulation
        - Find court decision on Cal-FIPPA cited above
    - FERPA
    - VPPA
    - TCPA
    - ….

Conclusion:

- In what areas are States pre-empted from enacting data protection regulations and what is the impact of such pre-emption in terms of ability to become "adequate" via enacting comprehensive data protection regulations?

What process would a State have to follow to obtain Adequacy?

Applying for Adequacy:

Can a US State apply for adequacy?

- An adequacy determination is not an international agreement
    - What would be the nature of the application/granting procedure? Is this an international treaty? Other?
    - What is the autonomy of a State to negotiate with the European Union an "adequacy" finding?
- US State adequacy application would not violate the US constitution
    - Research

Consideration of application by the European Commission:

Obtaining Adequacy

Maintaining Adequacy

Conclussion

-

[i] EU Commision website https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en