Data Protection Committee Report
Checklist for Brand Owners

Issues to Consider when Evaluating a Data Protection Framework

Introduction

Since the European Union's General Data Protection Regulation (GDPR) went into effect in 2018, there has been a global proliferation of new laws and regulations in which governments seek to hold private companies accountable for protecting the personal data of their customers ("Data Protection Laws"). If companies are not compliant with the terms of these Data Protection Laws, they can be subject to significant fines, as well as the loss of customer goodwill, reputational damage and trust in the brand.

Trademark professionals, tasked with the job of protecting companies' brands, should be aware of Data Protection Laws. To this end, INTA's Data Protection Committee has created this checklist, is intended to support trademark professionals in identifying and evaluating the key issues to consider when addressing Data Protection Laws for their clients or companies.

This checklist is not a data protection standard or industry code. It is intended to be a tool for trademark professionals to help identify relevant issues. Data Protection Laws are changing rapidly and this checklist should be viewed only as a starting point. It is important, given the dynamic nature of Data Protection Laws, that trademark professionals conduct further research on the specific laws and regulations of the country or countries in which their company/clients operate.

Disclaimer

This checklist is a multijurisdictional tool developed to assist brand owners and trademark professionals. It is not intended to create or be used as a data protection standard or industry code.

DATA PROTECTION TERMS

Definitions

Cookies

The cookie is a type of file that stores user information and is sent by a website through a browser. This file is downloaded on computers, tablets, cell phones or any other device, in order to store data that may be updated or recovered by the person responsible for their installation.

There are several types of cookies, which can be classified in different ways according to the time in which they remain activated and according to their purpose:

- ✓ ***Own cookies***: those cookies that are sent to your computer from the owner of the website on which the user is browsing.
- ✓ ***Third-party cookies***: those cookies that are sent to your computer not by the owner of the website, but by third parties [1].
- ✓ ***First party cookies***: those cookies set by the website you are visiting. Only that website can read them.
- ✓ ***Session Cookies:*** those cookies that exist only during an online session. They disappear from your computer when you close your browser or turn off your computer. Companies generally use session cookies to allow their systems to uniquely identify you during a session or while you are logged into their website. This allows them to process your online transactions and requests and to verify your identity, after you have logged in, as you move through their website.
- ✓ ***Persistent Cookies***: those cookies that remain on your computer after you have closed your browser or turned off your computer. These cookies are typically used to track aggregate and statistical information about user activity.

Cookies can serve various purposes. Some jurisdictions restrict the use of cookies, depending on their purposes.

Cookie Policy

A written public document that provides website or application users or visitors with information on the cookies that are being used, the types of cookies and how they are used, the user data that the cookies track, where the data is sent, how the website and application owner manages tracking and privacy, and how the website users may control the cookies settings or opt out.

Data Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. A decision maker about what data is processed, how and for what purposes.

Data Processor

[1] Source: Uruguayan Data Protection Authority (URCDP). Cookie and profiles guide.

Any individual or organization providing a data processing service to others by receiving instructions on how data is processed and used and acting in accordance with such instructions.

Data Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[2]

Data Processing / Sharing Agreements

Agreements with processors/vendors to address their obligations to the organization and its customers of: data protection and security standards, cooperation, notice and liabilities in instance of a breach.

Data Protection Authority (DPA)

National/ Regional supervisory authority which has regulatory oversight concerning the processing of personal data because: (a) the controller or processor is established in the jurisdiction of the national supervisory authority; (b) data subjects residing in the jurisdiction of the supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that national supervisory authority.

Data Protection Impact Assessment (DPIA)

An assessment to identify and minimize data protection risks; it involves the analysis of systems, processing activities, and controls. It is a key part of accountability obligations under the GDPR and relevant data protection laws and helps to demonstrate compliance with data protection obligations.

Data Protection Officer

Person named by the Data Controller or Data Processor to act as a channel of communication between the controller, the subjects of such data and the DPA. The DPO's main role is to guide and advise the Data Controller/ Data Processor on data protection issues to ensure data protection compliance.

Data Retention Policy

A document which sets and explain the criteria for how long personal data should be stored and/ or archived by an organization and how it should be disposed**.**

Data Subject

An identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

[2] California uses the term "business" for controller and "service provider" for processor.

data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Transfer Impact Assessment

A risk assessment made prior to the transfer of personal data from the EU/EEA to Third Countries which are not subject to an adequacy finding by the European Commission (EC).[3]

Incident Response Plan

A plan designed to manage a data breach when it happens. The plan includes: (i) identifying the people who must be part of the decision tree to be contacted to address the breach (including a crisis management organization if available); (ii) mapping the geographies affected by the breach and the respective obligations in those countries or states; (iii) reporting within the legally required time frames,(iv) reporting to relevant parties such as the appropriate DPA, law enforcement, data subjects, regulators and insurers; (v) reporting the required information (e.g. scope of breach, data that was revealed and (vi) the steps taken to rectify any deficiencies that played a part in the breach and its consequences.

Information Security Policy

A document that safeguards the use and access to personal data by setting the parameters for authorized access and distribution of personal data.

International Data Transfer

Transfer of personal data to another jurisdiction.[4]

Joint Controller

Data controllers with common objectives or shared sources for the data being processed.

Lawful Basis

A lawful manner of processing an individual's personal data in a fair, clear and transparent way, in line with principles of lawfulness and accountability[5].

Personal Data

[3] The data exporter must assess, on a case-by-case basis, whether the exported personal data will be adequately protected in the Third Country, despite the Third Country not having been confirmed by the EC to provide an adequate level of protection. This requirement mainly follows the European Court of Justice's (ECJ) "Schrems II" judgment of July 2020. The new Stand Contractual Clauses (SCC) published by the European Commission in June 2021 expressly include this obligation in Clause 14.

[4] Data transfers between Member States of the European Union are not considered as International Data Transfers because of the unitary high level of protection in all EU Member States.

[5] See for example Article 6 of the GDPR which explains the lawfulness of processing. Under the GDPR, all processing activities must be justified by at least one of the six possible lawful bases, which are: consent from the data subject, in order to perform a contract, to comply with a legal obligation (not a contractual obligation), vital interests (e.g. to protect a life), public tasks (e.g. tasks of a public authority set out in law), legitimate interests (e.g. use of a person's data in ways they would reasonably expect and with minimal invasion of privacy).

This term may vary by jurisdiction. Under GDPR it means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Under a number of US state privacy laws, it means any information that is linked or reasonably associated to an identified or identifiable natural person.

Personal Information

This is a term used by certain jurisdictions rather than "personal data." The definition varies by jurisdiction. For example, under the California Privacy Protection Act, personal information is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Privacy Notice

A public document published by a data controller or a processor which includes detailed information about its processing of personal data in a specific, clear and transparent way. It usually includes not only information about the identity of the controller/processor, the types of personal data which are being processed, the purposes and legal basis for the processing, recipients of the data etc. but also informs the individuals about their rights (such as the right to request information, correction, deletion, to lodge complaints etc.). Privacy Notices are used, for example, on websites or as attachments to contracts.

Sale of Data

Any sharing or disclosure of personal information or personal data for monetary considerations and under some laws for any "valuable" consideration.

Sensitive Personal Information

A subcategory of personal information that is usually subject to additional restrictions, including the obligation to obtain consent. Examples of such information include personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status or trade union status; the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; the personal data collected from a known child; or precise geolocation data.

Targeted Advertising

This means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests[6].

[6] A number of US laws require controllers to provide an opt-out from such advertising.

The following checklist is divided into subtopics for your consideration.

I. Type of Personal Data Processed by the Brand Owner

1. Identify the primary function of your organization.
2. Determine whether your organization processes personal data.
3. Identify the types of data that your organization collects, processes and retains.
4. Determine how your organization collects data, including personal data (e.g., devices, direct on website, through third parties).
5. Determine whether your organization handles any special categories[7] of data (e.g., health data, financial data or data relating to criminal convictions and offenses).
6. Determine whether your organization processes children's data. Special laws may apply in your jurisdiction to the handling of children's data such as:
    - requirements to obtain and verify parental consent
    - requirements to communicate privacy information in a manner that a child[8] would understand.
7. Determine whether your organization has processes in place to apply the right laws to processing (or avoiding processing) children's data in different jurisdictions
8. Determine whether your processing operations constitute automated decision making or profiling. In some jurisdictions, additional requirements may apply to these types of processing operations (e.g. information on the use of automated decision making or profiling, consent to this use or requirements for review by a natural person of the results of automated decision making).

II. Data Mapping and Documentation

9. Determine whether your organization maps the flow of its data. For example, does your organization map where it hosts data, whether in the cloud or on servers on your premises?

[7] Please note that the definition of personal sensitive data or special categories of data varies from jurisdiction to jurisdiction.

[8] Jurisdictions also have different rules on who they regard as a child.

10. Determine whether your organization has and maintains records explaining the type of data it handles and how the data is handled, processed, retained and destroyed[9].

11. Identify the "Lawful Basis" applicable to your organization's data processing.

12. Confirm whether your organization needs to and has carried out a DPIA.[10]

III. Data Minimization

13. Determine whether the personal data which your organization collects from consumers is limited to what is "adequate and relevant" as clearly stated to the consumer in advance of the collection (i.e., limited to what is necessary to achieve the purpose for which it is collected and/or processed). There must be a justifiable reason to retain the data for longer periods

14. Ensure that your organization does not collect or retain any more personal data than is necessary to achieve the legitimate purposes for which the data was collected.

IV. Data Protection Officer

15. Determine whether your organization is required by law to have a DPO. There are different criteria which will apply based on different jurisdictions. For example, the number of employees in your organization and the types of data your organization processes may be key factors.

16. Identify who is acting as the data controller and who is acting as the data processor in each of the organization's business relationships[11].

V. Accountability

17. Determine how your organization communicates to customers and how it uses their personal data. Your Privacy Notice should satisfy applicable legal requirements. Although these requirements will vary, the privacy notice, for example, should explain:

---

[9] Please note that Article 30 under the GDPR requires maintaining such records.

[10] The DPIA is a key part of accountability obligations under the GDPR and relevant data protection laws and helps to demonstrate compliance with data protection obligations.

[11] Article 30 under the GDPR requires that you maintain a list of processors who handle personal data on behalf of your organization.

- what data is collected and used and why
- what data transfers take place and why
- how customers can exercise their rights relating to their data
- and who customers can contact if they have any questions or complaints.

18. Determine which data protection authorities have jurisdiction over your organization.[12] Applicable Data Protections Laws need to be examined to determine which authority or authorities have jurisdiction.[13]

19. Determine whether your organization's Privacy Notice is concise and easily accessible and uses clear and plain language.

20. Determine whether your organization's Privacy Notice identifies how your organization secures personal data.

21. Determine whether your organization has a consent management program in relation to direct marketing. You may require a system or software that tracks the withdrawal of consent to ensure you no longer market to those who have requested that they no longer be contacted by your organization. Some browsers have a "do not track" feature that lets users tell websites that they do not want to have online activities tracked, so ensure your organization responds to browser "do not track" signals.

22. Determine whether your organization has a Document Retention Policy or process in relation to the storage and deletion of data.

VI. Technical, Administrative and Security Measures

23. Determine whether your organization has technical and security safeguards in place in relation to the handling of data internally and externally. This may involve conducting security audits and establishing IT policies for the protection of data. If your organization handles sensitive or personal data it should have internal procedures to manage this. Your organization may wish to consider ISO certification or an equivalent.

24. Determine whether your organization has administrative safeguards in place in relation to the handling of data. You should know how your organization reports internal breaches and what is the chain of reporting. Identify whether your organization engages a third party to monitor potential breaches and whether your organization keeps a log of reported or addressed breaches.

[12] Please note that different laws provide for extraterritorial application, meaning that they might be applicable even if you are not present in that country (as for example GDPR).

[13] You may have to register your organization or your processing activities with one or more authorities.

25. Determine whether your organization integrates data protection in its processing activities.

26. Determine whether your organization take steps to anonymize or pseudonymize data.

VII. Organizational Risk Management and Data Breach Response

27. Identify an internal risk management committee or a body which specifically addresses data or security issues such as an Information Security Management Committee (ISMC).

28. Determine whether your organization has an Incident Response Plan (i.e., the plan for how it will handle a data breach when it happens) that lays out:

a. the people who must be part of the decision tree to be contacted to address the breach (including a crisis management organization if you retain one)

b. reporting within the legally required time frames

c. reporting to relevant parties such as the appropriate DPA, law enforcement, data subjects, regulators and insurers

d. reporting the required information

i. scope of breach

ii. data that was revealed

iii. steps the organization is taking to rectify the breach

iv. mapping the geographies affected by the breach and the respective obligations in those countries or states.

29. Determine whether your organization conducts tabletop exercises for incident response (i.e., practicing mock incident with the needed stakeholders in the ISMC or a broader identified group of personnel listed in the Incident Response Plan).

30. Determine whether your organization has an Information Security Policy and corresponding security measures in place.

VIII. Training and Awareness

31. Determine whether your organization has formal training for employees to educate them about data security, data protection laws, and your organization's requirements, policies and procedures.

32. Determine whether your customers require your organization to provide data protection and privacy training for your employees/contractors, usually through the

request for proposal process and/or through annual compliance questionnaires that they send the organization.

33. Determine whether your customers require your organization to assure that any subcontractors used in providing their goods/services meet data protection and privacy awareness levels.

34. Determine whether your cyber or related insurance carrier requires that you train your employees/contractors in data protection and privacy.

IX. Internal Operations

35. Identify the people in your organization who are responsible for handling data and data systems and determine whether they understand the difference between:

- data subjects
- data controllers
- joint controllers (with common objectives or shared sources for the data being processed)
- data processors.

36. Determine whether they have performed an evaluation of these roles and how it interacts with data in relation to: consumers, customers and related entities and vendors.

37. Determine whether your organization is a joint controller with another organization, client or vendor. For example, for data on the participants in a webinar, the webinar organizer may be a joint controller together with the webinar sponsor.

X. Contracts with Third Parties

38. Determine whether your organization's client contracts address data protection and have data protection provisions.

39. Determine whether your organization is a data importer or a data exporter in relation to customer data collected and transferred under its contracts and in the provision of its goods/services.

40. Determine whether your organization's vendor contracts address data protection. Identify any data processing / sharing agreements with vendors who access or process personal information on behalf of your organization (to address their obligations to you and your customers of data protection and security standards, cooperation, notice and liabilities in instance of a breach).

XI. Data Disclosure

41. Determine whether your organization has a policy or process in place to handle subpoenas and other requests from law enforcement and private parties (such as cybersecurity professionals and intellectual property rights holders) for the disclosure of non-public personal data.

XII. International Data Transfers

42. Determine whether your organization transfers personal data across international borders between internal group companies or to or from customers, suppliers or service providers.

43. Identify any data protection mechanisms such as standard contractual clauses that your organization relies on to assure legal compliance and security for the transfer of data internationally. Conduct a Data Transfer Impact Assessment where necessary.

44. Evaluate if your business is located in or does business in a country or countries that are recognized as having adequate protection for personal data transfers under the GDPR.

45. Review clients/customers/suppliers/service contracts to see if they address international data transfers.

XIII. Data Subject Rights

46. Determine whether your organization has a way for applicants, employees, clients, customers or third parties to exercise the rights recognized to them by applicable laws regarding information your organization has collected about them.

47. Determine whether your organization has data portability procedures, so that if a third party requests that their data be returned to them or transferred to someone else your organization can address this request?

48. Determine whether your organization has the administrative capability to address a request to correct inaccurate data.

49. Determine whether your organization has the administrative capability and procedures in place to handle requests from individuals for details of information that you hold about them. If it is too burdensome, you should consider engaging a third party provider or utilizing third party software to help with these requests.

50. Determine whether your organization has a method for validating a data subject's identity to ensure the person making the request is authorized to exercise rights with respect to that data.

XII. Cookies

51. Identify any Cookies on your website.

52. Create a Cookie Policy.

53. Determine whether your organization has a Cookies banner and clearly and transparently identify to visitors to your website the Cookies on the site and provide them the ability to accept all or some of the Cookies.

54. Determine how your organization tracks Cookies to prove compliance.

END OF CHECKLIST

Published: February 22, 2023