Transatlantic Data Privacy Rules (TDPR) Codebook

Contents

METHODOLOGY

How were the documents collected?

- This database includes publicly available regulations in Europe and the United States relating to e-commerce and data protection. The concept of regulation was understood in a broad sense and includes laws, directives, guidelines, codes of conduct and private requirements. The mere explanation of the sense of a law or a code was however not considered to be a regulation by itself.
- Documents only dealing with technical matters of operating a website (e.g.: server security or web architecture) were excluded. This database only focuses on data protection rules, not technical standards.
- Both public and private regulations in the transatlantic area were included.
- The laws or regulations of U.S. federal states or EU member states were not included.
- Similarly, only the regulations adopted by private associations operating at the EU level (or in more than one European country) or US level were included. Private associations only active in one EU member state or one U.S. federal state are not part of this database.
- Regulations adopted by transnational private associations were included.
- To access and download older versions of private regulations, the digital archive *Wayback Machine* was used. This archive made possible to collect almost all documents put forward by private associations in the transatlantic area since 1995.
- Documents included in this database span from 1995 to today (August 2017). The choice of 1995 as a starting date reflects two main developments in the regulation of e-commerce. First, 1995 can be considered as the year of inception of e-commerce as we know it today. In that year, the National Science Foundation privatized the NSFNet and eliminated the acceptable use policy which impeded the network's use for commercial purposes. The collection of personal data by private companies significantly expanded following this decision. Second, the European Union also adopted its first directive on data protection in 1995.

What counts as a "rule"?

- Rules are standards of behavior followed, voluntarily or not, by an actor.
- Rules can have a high degree ("must", "shall", "will", etc.) or low degree ("may", "could", "encourage") of commitment.
- Rules can be found in a single sentence or an entire paragraph. Similarly, a rule can be really detailed or really broad.
- Rules cannot be found in the preamble, the foreword or the explanatory memorandum of a regulatory documents. The explanatory memorandum can however be used to clarify the meaning of a rule.
- The definitions and the objectives were also not considered as rules.
- Rules can be repeated many times in the same regulatory document. Those repetitions do not need to be found in the same parts of a regulation.
- Vague reference to another article or part of a regulation were not coded.
- Similarly, it is not assumed that a general reference to another regulation means that an actor adhere to all the rules of that regulation. It will only be coded when it is clearly mentioned that the actor will apply the rules put forward in the regulations.

What counts as "data protection"?

- Data protection broadly refers to measures taken to insure that personal data are safeguarded against any wrongful actions.

- "Personal information" are understood as a synonymous of personal data.

- Rules aiming to protect "data privacy" are also included.

- This database only focuses on data controller's obligations towards data subjects and on data subject's rights vis-a-vis data controllers. Data controllers' obligations towards states or states' obligations towards data subjects were not coded.

- Importantly, this codebook uses a terminology (“data subjects”, “data controllers”, “data protection”, etc.), which is traditionally used in Europe. This however does not reflect any personal preference for an EU model. It is moreover not intended to exclude rules using another terminology, such as the American one (“individuals”, “consumers”, “privacy”, etc.). This codebook aims to compare the extent to which rules on “data protection” or “data privacy” are substantively similar, not how similar their terminology is.

CODING RULES

01. Transparency

- Broadly refers to data controllers' obligations to clearly inform and notify data subjects of their data collection practices.

- Include data controllers' obligation to publish a "privacy notice", "privacy policy", "privacy statement" or "policy content".

- Include data controllers' obligation to follow an openness principle and inform data subjects of their online practices.

- The content of the privacy policies or the nature of the information that data controllers must give to data subjects should be coded in their respective nodes.

01.01 Privacy statement

- Include the obligation for data controllers to publish a privacy notice or statement on their website.
- Include any mention that a data controller should broadly inform or describe its privacy practices to data subjects.
- Include the obligation for data controllers to have a privacy notice, which is clear, conspicuous and/or easy-to-read.
- Include the obligation for third parties to provide notice on their own website. However, the obligation for data controllers to inform data subjects that third parties collect their personal data should be coded in node 01.09.
- Exclude the obligation to provide information with the aim to educate consumers (see node 15). Only code here the obligation for data controllers to inform data subjects or their consumers of their own privacy practices.

01.02 Data controller's identity

- Include the obligation for data controllers to inform data subjects of their identity.
- Include any rules stating that data controllers must provide their contact information in their privacy notice or statement.

01.03 Data types and purposes

- Refer to the obligation for data controllers to inform data subjects of the types and purposes (or nature) of data affected by their data collection or processing practices.
- Include rules requesting data controllers to say how they will use personal data.
- Include the obligation for data controllers to indicate that no personal data is collected or that some types of personal data are excluded from their data collection and processing practices.

01.04 Data source

- Include any rules requiring data controllers to inform data subjects of the source of their data.
- Include the obligation for data controllers to inform data subjects when they merge their data with personal data collected from other sources.
- Include rules indicating that data controllers cannot prohibit other controllers or users of personal data to inform data subjects that they are the ones which originally collected their personal information.

01.05 Data retention time

- Include any rules stating that data controllers must inform data subjects of how long their personal data will be kept.
- Also code here the obligation for data controllers to reveal how do they determine the data retention time.

01.06 Third-party transfer

- Include rules providing that data controllers must inform data subjects that their personal data might be shared or disclosed with third parties.
- Include rules requesting data controllers to disclose with whom they share personal data.

01.07 Third-party transfer safeguards

- Include the obligation for data controllers to inform data subjects of which safeguards are implemented by third parties with which their personal data is shared or disclosed.

01.08 Third-party collection

- Include the obligation for data controllers to inform data subjects that third parties may collect personal data on their website.
- Include rules indicating that third parties must post an enhanced notice on the website where they are collecting personal data.

01.09 Automated or passive data collection (Cookie notice)

- Include the obligation for data controllers to inform data subjects that they may be subject to passive or automated data collection techniques (e.g.: cookies).

01.10 Consequences of withholding personal information

- Include any obligations of data controllers to inform data subjects of what consequences are entailed from their decision not to disclose their personal data.

01.11 Policy change

- Include any rules providing that data controllers must notify or inform data subjects of any policy change.
- Also include rules providing that data controllers must obtain consent before applying any policy change, even though it is not clearly written. It is implicitly understood that data subjects will have to be notified to be able to provide consent.

02. Consent

- Refer to any rules pertaining to the obligation for data controllers to obtain the consent of data subjects before collecting and processing their personal data.
- Include both opt-in and opt-out approaches. Opt-in approaches are situations where the data subjects must take affirmative steps to allow data collection or processing practices. As opposed, opt-out approaches are situations where the data subjects must take affirmative steps to prevent data collection or processing practices.

02.01 Original consent

- Refer to the obligation for data controllers to obtain the consent of data subjects, either implicitly (opt-out) or expressly (opt-in), before collecting and processing their personal data.
- Include the obligation for data controllers to provide data subjects with choices with regards to the collection and use of their personal data.

- Include the obligation for data controllers to obtain consent before using personal data for secondary uses (i.e. use unrelated to the original transaction. However, exclude rules requiring to obtain consent before using for purposes other than that for which they were originally collected. See 02.02 and 04.01.
- Also code here any mentions that data controllers should respect the choices or wishes of data subjects.

02.02 Consent renewal

- Include any rules requiring data controllers to renew consent after having changed their privacy policy.
- Include any rules indicating that data controllers must treat personal data according to their original privacy policy to which data subjects have consented until they are able to renew their consent.
- Include any rules stating that data controllers can only use personal data in ways compatible with their original policy except if they obtain the data subject's consent. Also code this rule in 04.01.

02.03 Consent withdrawal

- Refer to the possibility for data subjects to withdraw their consent to the collection or use of their personal data. It can either be for implicit or explicit consent.
- Include the possibility to withdraw consent for data transfer.

02.04 Cookie consent

- Refer to the obligation for data controllers to obtain data subjects' consent or provide a choice to data subjects before storing cookies on their computer. The obligation to obtain consent before storing information on a data subject's computer, even when there is no mention of cookies should also be coded here.
- Include the obligation for data controllers to obtain data subjects' consent before automatically harvesting/collecting all URLs traversed by a particular computer.

02.05 Third-party collection and use consent

- Refer to the obligation for data controllers collecting and using personal data from third-party websites to gain consent or offer choices to data subjects.
- Do not confuse with the obligation to obtain consent before sharing personal data with third parties. Only code here the obligation for a party collecting personal data own the website of another party to still allow data subjects to make choices or give consent. This obligation is often linked with rules on Online Behavioural Advertising (OBA).

02.06 Right to refuse automated decision-making

- Refer to the obligation for data controllers to respect the choice of data subjects not to be subject to decisions solely based on automated data processing.

02.07 Right to object

- Refer to the obligation for data controllers to offer data subjects the possibility to object to the use of their personal data. This rule should not be confused with to obligation to offer choices to the data subject. Most notably, do not code here the obligation to allow data subjects to opt-out at anytime. Only code here, the obligation for data controller's to allow data subjects to object to the use of their personal data when it is not based on his consent (i.e.: legitimate interests or public interests).

03. Collection limitations

- Refer to rules requiring data controllers to minimize data collection to what is necessary for specified and legitimate purposes.
- Exclude mere indication that privacy policies must inform individuals of their data collection practices. Code as a transparency measure.
- Exclude data controllers' obligation to collect personal data that is relevant to fulfill legitimate purposes. See 06.02.

03.01 Purpose limitation

- Include the obligation for data controllers to only collect personal data that is necessary for the specified purposes.
- Include the obligation for data controllers to only collect personal data for legitimate purposes.
- Include the obligation for a data controllers to limit their collection practices to data appropriate to their business (e.g. marketing or sale).
- Include the obligation stating that data controllers should limit their collection practices to data relevant for their specified purposes.

03.02 Fair and lawful

- Include the obligation for data controllers to collect personal data in a fair and lawful way.
- Do not confuse with the obligation to *process* personal data in a fair and lawful way. This rule should be coded in 04.02, not here.

03.03 Third-party source

- Refer to the obligation for data controllers using personal data collected from third parties to verify that the latter collected the data in a legitimate way.
- Include the obligation to do due diligence when collecting personal data from third parties.

04. Use limitations

- Refer to any obligations limiting the use of personal data by data controllers.
- Exclude any limitations based on the special nature of personal data (sensitive data, children data, third-party collected data, etc.)

04.01 Original purposes

- Refer to any rules providing that data controllers should only use personal data as originally notified to data subjects.
- Include any obligations to only use personal data for one specific purpose (e.g.: marketing) or only in ways associated with a data controller's business.
- Include any rules requiring data controllers to not process personal data for new purposes, except with the consent of data subjects. Also code in 02.02.

04.02 Fair and lawful

- Refer to the obligation for data controllers to only use personal data in a fair and lawful way.
- Do not confuse with the obligation to *collect* personal data in a fair and lawful way. This rule should be coded at 03.02.

04.03 Right to restrict

- Refer to the possibility for data subjects to temporarily limit the use of their personal data by data controllers.

05. Disclosure

- Refer to any rules related to the transfer of personal data by data controllers to third parties.
- Include the obligations of data controllers regarding cross-border transfers and the sale of personal data.

05.01 Sharing with independent controller

- Refer to any obligations related with the transfer of personal data from a data controller to an unaffiliated third parties.

05.01.01 Consent

- Code here the obligation to obtain the consent of data subjects before transferring their personal data to third parties.
- Include the obligation to offer a choice to data subjects before transferring their personal data.
- Include the right of data subjects to refuse that data controllers share their personal data with third parties. This is considered to be equal to an opt-out form of consent.

05.01.02 Adequacy of third-party policies

- Refer to the obligation for data controllers to verify the adequacy of third parties before sharing with them personal data.
- Include any rules requiring data controllers to share personal data with third parties which provide substantially similar privacy protections. The obligation to otherwise inform data subjects if their personal data is transferred to third parties without sufficient privacy protections should also be coded here.
- Include the obligation for data controllers to share their privacy policies with third parties with which they are sharing personal data.
- Include the obligation for data controllers to have an agreement providing an equivalent level of protection to their privacy policy with third parties should both be coded here and in 05.01.03.

05.01.03 Contract

- Refer to the obligation for data controllers to have have an agreement or contract with any third parties with which they share personal data.
- Include any mention that a data controllers should “contractually” require that a third party receiving personal data should abide by its policies.
- Include the obligation that the contract specifies that the data controller remains responsible for the use of its collected personal data.

05.01.04 Remedial actions

- Refer to the obligation for data controllers to take remedial actions against third party which receives personal data. It is often based on a contract that the data controller should have established with the third party.

05.02 Sharing with joint controller

- Refer to any rules defining how two or more data controllers which jointly manage personal data should operate.

05.03 Sharing with processor

- Refer to any obligations of data controllers when sharing data with processors or service providers, i.e. third party companies employed to specifically analyze the data for the data controllers.

05.03.01 Use limitations

- Refer to the obligation for data controllers to ensure that processors will only process under the instruction of the data controller.
- Include any rules indicating that a processor should not hire another processor without prior authorization from the data controller. Also code here the obligation that this second processor should respect the same obligations than the first one.

05.03.02 Adequacy of processor policies

- Refer to any obligations of data controllers to ensure that processors respect the same level of protection that they offer.
- Include any rules stating that processors must respect the privacy policy of the data controller and keep personal data confidential.
- Include any mention that processors must maintain a level of security equivalent to the one of the data controller.

05.03.03 Contract

- Refer to the obligation for data controllers to have a contract or an agreement when sharing personal data with a processor or service provider.
- Importantly, if it is indicated that the contract should foresee that the processor or service provider must respect the privacy policy of the data controller or only use personal data under its instruction, also code in 05.03.01 and 05.03.02.
- Include the obligation that the contract specifies that the data controller remains responsible for the use of its collected personal data.

05.04 Third-country transfer

- Include any obligations that data controllers must specifically respect when transferring personal across borders.

05.05 Prohibition to transfer prospect information

- Refer to the obligation for data controllers not to share personal data collected indirectly, i.e. personal data on a data subject collected through another one.

06. Data quality

- Refer to rules aiming to ensure that personal data collected by data controllers is of quality.
- Include the obligation for data controllers to ensure that personal data they collect is accurate, complete and kept up-to-date.
- Include any obligation for data controllers to develop procedures to maintain the accuracy of personal data.
- Any mention that data controllers should allow data subjects to access their personal data to ensure they remain up-to-date should both be coded here and at 07.01.

07. Individual participation

- Refer to the ability of data subjects to control how their personal data is used and shared.

07.01 Acces and review

- Refer to the possibility for data subjects to access and potentially review personal data that a data controller has on them.

- Include the obligation for data controllers to ensure that data subjects are able to determine whether a data controller holds information on them. Similarly, the obligation for data controllers to confirm to data subjects if they hold personal data on them should be coded here.
- The obligation for data controllers to ensure data quality by providing data subjects with an access to their personal data should be coded here and at 06.01.
- Also code here rules providing that data subjects may correct their personal data if no rules specifically indicate that a data subject may access its personal data. It is implicitly assumed that to be able to correct its data, data subjects will be given access to its personal data.

07.02 Correct

- Include any rules providing that data subjects may correct, rectify or change the personal data that a data controller has on them.

07.03 Erasure

- Include any rules providing that data subjects may request the erasure, suppression or blocking of inaccurate personal data.

07.04 Notification of third parties

- Include any rules providing that the data controller should inform any data recipients of changes to the personal data of a data subject.

07.05 Access denial

- Code here any rules requesting data controllers to explain to data subjects why a request for access, correct or remove personal data has been refused.

07.06 Right to challenge

- Include any rules allowing data subjects to challenge any decision by data controllers to deny access requests.

07.07 Right to be informed of automated practices

- Include the obligation for data controllers to inform data subjects of the existence and logic behind their automated processing practices.

07.08 Authentication

- Include the obligation for data controllers to verify the identity of a data subject before giving him/her access to personal data.

07.09 Not unduly limit

- Include the obligation for data controllers to not create any unnecessary barriers for data subjects to access, correct and delete their personal data.
- Include any obligation stating that access to personal data should be free or should not cost more than a specific price.

07.10 Data portability

- Include any rules providing that data subjects may request to receive their personal data in portable format. Do not confuse this rule with the possibility to have access to its personal data. Only code here, rules specifically requesting that the personal data may be shared in a portable format (i.e. in a format, which can easily reused by another data controller).

07.11 Right to be forgotten

- Include any rules providing that data subjects may request the erasure of personal data no longer necessary for the purposes they were collected.

07.12 Right to representation

- Include any rules providing that data subjects may mandate a non-profit to represent them in remedial proceedings.

08. Sensitive data

- Refer to any rules which specifically apply to the protection of sensitive data.
- Sensitive data include information. While the definition of sensitive data may differ, it generally includes data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sexual orientation.

08.01 Consent

- Include any rules providing that data subjects must give their consent before sensitive data may be collected and/or processed by data controllers.
- Include rules that only apply to one type of sensitive data (e.g. health data or financial data).
- Also code here any indication that sensitive data require a "higher" level of choice than non-sensitive data.

08.02 Third-party transfer

- Include any rules that a data controller must request data subject's consent before sharing personal data with any third parties.
- Rules indicating that a data controller should use encryption or any other security measures when sharing sensitive data should not be coded here, but in 08.03.

08.03 Special security measures

- Include any rules indicating that data controllers should adopt security measures specifically designed to protect sensitive data.
- Include rules requesting data controller to use encryption to protect sensitive data, either when storing or sharing them.
- Include rules providing that data controllers should adapt their security measures to the level of sensitivity of personal data.

09. Children data

- Refer to any rules which specifically apply to the protection of children data. The different age used to determine who is a children is not considered.

09.01 Special notification

- Include any rules providing that data controllers must provide a special notice for the collection and/or process of children data.
- Include rules indicating that data controllers should notify children when they leave their website for another one which may not use the same privacy policy.
- Include any rules requiring data controllers to provide any type of information (e.g. data source, potential use, etc.) on their data collection and processing practices relating to children data.

- Rules calling for data controllers to notify data subjects of their rights and obligations should be coded here and in the other nodes applicable.
- The obligation to use “awareness tools” when dealing with children on their website should be coded here.
- Parental notifications should also be coded here.

09.02 Special collection limitations

- Include any obligations of data controllers to limit their data collection practices with regards to children.
- Include the obligation for data controllers to remind children of not posting online personal data.
- Include the obligation for data controllers to not condition a children participation in an activity online on the condition of giving his/her personal data.
- Include any rules indicating that children data may not be collected for a specific purpose.

09.03 Parental control

- Include any rules requiring data controllers to encourage parents to get involved an monitor their children’s online activities.
- Include any rules pushing data controllers to encourage parents to use the adequate technology and software to protect the privacy of their children online.
- Include any rules indicating that data controllers should inform parents about ways to protect the privacy of their children online.

09.04 Parental consent

- Include the obligation for data controllers to obtain parental consent before collecting, using and/or processing children data.
- Rules providing that data controllers should allow parents to refuse further use of their children data.

09.05 Parental access

- Include any rules providing that parents may access the personal data of their children.
- Include any rules allowing parents to request that their children data be corrected or removed.

09.06 Third-party transfer

- Include any rules providing that data controllers must provide specific information to parents when sharing their children data with third parties.
- Include any rules requiring parental consent before any children data may be transfered to third parties.

09.07 Automated collection practices

- Include any rules requiring specific measures when using automated practices (cookies, web beacons, etc.) to collect children data.

09.08 Special security measures

- Include any rules stating that data controllers should adopt security rules specifically designed for children data.

10. Data security

- Refer to any rules requesting data controllers to implement security measures to protect the confidentiality of personal data.

10.01 Commitment to data security

- Refer to any rules specifying that data controllers should develop an environment conducive to data security.
- Include broad statements that data controllers should take reasonable precautions, maintain a written data security policy and adopt control measures.
- Importantly, rules foreseeing that security measures must be proportional to the sensitivity of the personal data being collected or processed should be coded in 08.03.
- Include rules providing that data controllers must use specific techniques like notably encryption, firewall, safe servers or VPN to protect personal data.
- Include rules asking that data controllers take measure to protect themselves against virus or malicious codes. However, do not code here rules providing that data controllers should refrain from introducing virus or malicious codes on the computer of data subjects. This is not considered to be a data protection measure.
- Include rules requesting that personal data may not be accessible to any people. However, rules providing that personal data may only be accessed by a data controllers' employees with a legitimate business reason should be coded in 10.02.
- Include rules stating that data controllers must establish physical, electronic and administrative security measures.
- Include rules indicating that data controllers must adopt security measures of a physical nature (e.g. locks, secured rooms, etc.)

10.02 Anonymization or Pseudonymization

- Include any rules requiring that data controllers anonymize or pseudonymize the personal data that they have collected and processed.
- Exclude rules stating that "de-identified" or "anonymized" data is considered to be non-personal information. Only include rules that indicates that anonymiation or pseudonymization should be used when possible.
- Exclude rules requiring that data controllers adopt encryption or other technical measures to protect personal data.
- Exclude rules that require data controllers to destroy or *anonymize* when the personal data is no longer needed. See node 11 instead.

10.03 Access control

- Include any rules limiting access to personal data to employees who "need to know" based on their job responsibilities.
- Exclude any rules stating that data controllers must prevent unauthorized access by external people or third parties. Similarly, exclude rules stating that only authorized users can access personal data. Instead code 10.01 as broad commitments to data security.

10.04 Record-keeping

- Include any rules providing that data controllers must keep a record of their processing activities or authorized users accessing personal data.
- Include any rules requiring that data controllers should keep a record of to whom they share personal data.

10.05 Review and monitor

- Include any rules requiring data controllers to regularly review and monitor their security measures.
- Exclude the obligation for data controllers to regularly check or demonstrate their compliance with their broad privacy policy. Code instead in 13.02.

10.06 Employee training

- Include rules providing that data controllers must provide training to their employees to ensure that they respect their privacy policy.

10.07 Privacy risk assessment

- Include any rules providing that data controllers must do a privacy risk assessment *before* processing personal data.
- Exclude any mention of annual or regular risk assessment of current security practices. Code in 10.05 as a review mechanism.

10.08 Data protection officer

- Include any rules requiring data controllers to designate an individual as accountable for the implementation of its privacy policy (i.e. data protection officer).
- Any mention that responsibility and accountability must be assigned to an employee should be coded here.
- Include rules indicating that a data controller must establish a contact point for privacy enquiry.
- Include rules requesting data controllers to name a chief privacy officer or engineer.
- Include rules indicating that data controllers should assign responsibility of ensuring the respect of their privacy policy to an individual or group of individuals.

11. Data retention

- Refer to any rules indicating that data controllers must not keep personal data for longer than necessary.

12. Data breach

- Refer to any rules requesting data controllers to take actions to prevent or resolve data breaches.

12.01 Privacy breach management policy

- Include any rules providing that data controllers should adopt a specific policy or procedure to deal with potential data breaches.
- Include the obligation to set up a readiness plan.
- Exclude obligations to notify data subjects or authorities, see 12.02 & 12.03.

12.02 Data protection authorities' notification

- Include any rules requiring data controllers to inform relevant data protection authorities of data breaches.

12.03 Data subjects' notification

- Include any rules requiring data controllers to inform all data subjects affected by a data breach.

13. Accountability

- Refer to any rules aimed at ensuring that data controllers comply with their own rules and remain accountable for their data practices.
- Include all rules related to complaint mechanisms.
- Exclude vague rules indicating that data controllers need to be accountable. Only code rules requiring the existence of specific accountability mechanisms.
- Rules indicating that responsibility or accountability should be attributed to an individual or group of individuals should be coded in node 10.08 as they are considered to be equivalent to name data protection officer(s).

13.01 Complaint mechanism

- Include any rules requiring data controllers to establish a complaint mechanism or join a dispute settlement program.
- Include rules requesting data controllers to inform data subjects that they can submit complaints with regards to the use of their personal data.
- Include any rules stating that data controller must establish a mechanism to appeal any decisions taken by the dispute settlement body.
- Include rules related to the possibility to have access to a remedy with the data controllers. But exclude rules indicating that data subjects retain the right to a remedy in front of national courts.
- Exclude rules stating that data controllers must allow data subjects to challenge decisions to refuse them access to their personal data. See instead 07.06.

13.02 Compliance mechanisms

- Include any rules stating clearly that the data controller must be able to demonstrate how it is accountable for his/her data practices. It may includes annual compliance review with its data policies, external audits, etc.

14. Education

- Include any obligation for data controllers to educate or teach data subjects about their data collection and data processing activities.
- Exclude rules requiring data controllers to educate its employees. See 10.05.