Digital Cooperation Organization

DCO PRIVACY PRINCIPLES

TABLE OF CONTENTS

Preamble

Access to and use of data is a key element of the digital economy and an enabler of international trade. This has made data governance central to any successful policy to support economic growth. Data governance requires regulation that enables access to data and creates trust amongst governments, businesses, employees and consumers who are online in increasingly interconnected ways.

The protection of personal data in the digital economy and international trade is essential in order to keep individuals in general and consumers in particular engaged, and to build and maintain trust that stakeholders who collect, process and use their information are considering and protecting their privacy. This is particularly crucial with the advent of emerging technologies, which enable unprecedented levels of personal data processing and analysis. Therefore, it is imperative for governments, entities, and organizations to establish and adopt robust privacy principles that provide a strong framework for responsible data collection and processing.

The DCO Privacy Principles articulated herein are intended to serve the purpose of setting a consistent standard for the protection of personal data. These principles shall apply exclusively to personal data, and they are designed keeping in view the specific challenges arising from the processing of personal data using emerging technologies including but not limited to Artificial Intelligence ("AI").

As a foundational framework governing the processing of personal data, the DCO Privacy Principles are an integral component of the DCO Interoperability Mechanism, which facilitates the trusted transfer of personal data among DCO Member States. Given that international trade and investments rely on seamless data flows as a fundamental component of doing business online, these principles establish a common basis to support participation in global supply chains and enable businesses to leverage data to add value to their operations. In this context, where the processing of personal data is governed by the DCO Privacy Principles, controllers and processors involved in international data exchanges must ensure that personal data transferred across borders are protected at the recipient's end in compliance with standards equivalent to those established by the DCO Privacy Principles.

Thus, the DCO Privacy Principles contribute to establishing a best practice basis of international data protection approaches, especially in the context of emerging technologies, by providing a robust yet adaptable data protection standard. These principles are not intended to serve solely as a mutual framework for DCO Member States; rather, they offer open, international guidance for any government or entity seeking to develop its data protection framework and related policies.

Also, the DCO Privacy Principles do not apply to the processing of personal data conducted in the course of personal, family or household activities that are unconnected to any professional or commercial undertakings.

1. DEFINITIONS

Text	Guidance / Commentary
Anonymization means Processing Personal Data in such a manner that the Individual is not or no longer identifiable with adequate means in the control of the processing person or organization.	The DCO Privacy Principles do not apply to the processing of anonymous data, including anonymous data for statistical or research purposes.
Controller means any natural person or legal entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.	The Controller may be a natural or legal person, public authority, agency or other body being able to hold their own rights under national laws. It includes persons or organizations who instruct another person or organization to Process Personal Data on their behalf. In case two of more Controllers determine jointly the purposes and means of Processing, this does not except them from each being individually responsible for the processing. The definition does not include Processors. The definition also does not include persons who Process Personal Data in the course of the Individual's personal, family or household activities and thus with no connection to a professional or commercial activity.
Fairness and Fair means that Personal Data is Processed only in ways that people would reasonably expect – considering changes in technologies and ongoing digitization – and not use it in ways that have unjustified adverse effects on them.	The Fairness principle shall protect Individual against inappropriate interference, e.g. from misleading practices, false pretenses, being hassled etc.
High-Risk Processing means any Processing of Personal Data that poses significant risks to the rights and freedoms of Individuals, while these risks can arise from the nature, scope, context, and purposes of the Processing. Risks are defined by the likelihood and severity of the harm threatened.	High-Risk Processing requires increased privacy and protection measures. The definition may e.g. comprise the Processing of very sensitive data like biometric data or genetic data. The High-Risk Processing can be further defined by the governments through their respective legal framework.
Individual means any natural person.	The definition clarifies that the DCO Privacy Principles only apply to data on natural persons and not to data from legal persons.

Text	Guidance / Commentary
Personal Data means any data about an identified or identifiable living Individual. Data does not constitute Personal Data if it is Anonymized.	The term comprises data about natural living persons. It does not comprise data about natural persons, who are not alive anymore (unless national law protects the data irrespective whether the person is alive or not) and not data about legal persons like corporates. Data about an identifiable Individual means any data, by which a natural person can be identified by reference to one or more identifiers such as name or identification number or factors specific to that person. It therefore also includes data that not by themselves alone, but when put together with other data allows identification of an Individual with adequate means in the control of the processing person or organization. For example, certain types of metadata, when aggregated, can allow identification of the Individual and, thus, altogether constitute Personal Data. On the other hand, data which are artificially generated and not produced by real-world events (synthetic data), are not Personal Data.
Processing means any operation or set of operations which is performed on Personal Data whether or not by automated means, including, for example, collection, use, transfer and disclosure of Personal Data.	Processing may include operations 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 of Personal Data. The Processing of Personal Data apart from automated means applies only to data which form part of a filing system or are intended to form part of a filing system. Filing system means any structured set of Personal Data which are accessible according to specific criteria, whether dispersed on a functional or geographical basis.
Processor means any natural person or legal entity, which Processes Personal Data on behalf of one or more Controllers.	The Processor is acting as the Controller's instrument or tool. The Controller remains responsible for the Processing by the Controller. The Processor may reside in the same country or in another country. In the latter case the Controller must consider any applicable data transfer requirements.

Text	Guidance / Commentary
Pseudonymization means a Processing by which personally identifiable data fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.	Pseudonymization has a consequence that Personal Data can no longer be attributed to a specific Individual without the use of additional data. The DCO Privacy Principles apply to pseudonymized Personal Data as the Individual is still identifiable. To benefit from Pseudonymization, such additional data must be kept separately and be protected by technical and organizational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person. This shall not jeopardize the accuracy and the data being correct for data processing and analysis.

2. LAWFULNESS AND FAIRNESS

Text	Guidance / Commentary
Personal Data shall be Processed lawfully. Processing is lawful if and to the extent that there is a legal basis for it. The legal basis may consist of: • the valid consent, which the Individual has freely given, • the contract with the Individual or a contract request - if and to the extent the Processing of Personal Data is necessary for its performance, or • a legal obligation and right to process Personal Data under national laws and regulations, considering the sensitivity of the Personal Data Processing.	A valid consent must be one that gives the Individual the right to make a decision without any undue influence. The Individual must be informed to which processing they consent – also as part of the transparency principle. Governments are at liberty to enact laws and regulations foreseeing or immanently involving the Processing of Personal Data. Governments may enact laws or regulations that e.g. foresee that Anonymization does not require a legal basis. The more sensitive the Personal Data is, e.g. classified as desiring a higher level of protection like health data, or religious beliefs, the more specific and narrow the laws and regulations should be, to govern its Processing. For instance, health data should be typically accessible in fewer, more limited cases than e.g., simple contact data. Also, children's Personal Data may be subject to stricter legal bases. Transferring Personal Data is also a type of Processing. A legal basis is also required if Personal Data is to be transferred to another person or organization. If the recipient resides in another country, the Controller must consider any applicable cross-border data transfer requirements.
Personal Data shall be Processed in a Fair manner respecting the Individual's rights and choices.	The Controller shall be honest about how the Personal Data will be used and Personal Data shall be used in ways that the Individual would reasonably expect. As part of the Individual's choice, Controller needs to respect the Individual's decisions in opting-out against certain communication sent by the Controller.
Automated decision making shall not be considered a Fair processing, if it involves high risks for the Individual's rights. In cases of high risks, there shall be human oversight integrated into the decision making.	Human oversight may be especially required with complex automated systems e.g. systems that have direct strong impacts on the Individual's rights and freedoms such as Artificial Intelligence.
Controllers may engage Processors with the Processing of Personal Data provided that such Processors implement appropriate technical and organizational measures to protect such data and provided that the Processors are contractually bound by the Controller to Process the Personal Data only according to the Controller's instructions.	To the extent the Processor Processes the Personal Data according to the Controller's instructions, the Controller remains responsible for complying with applicable privacy laws and regulations.

3. PURPOSE LIMITATION

Text	Guidance / Commentary
Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In determining whether a new purpose is compatible the initial purposes one key criterion shall be whether the extended usage stems from or is in furtherance of such purposes and what risks result for the Individual from such extended usage.	This principle limits collection of Personal Data to the purposes for which it is collected. Whether the Processing is lawful and fair, is to be decided for this specific purpose only. A purpose is legitimate if it is allowed or protected by national law, either derived from the constitution or bill of rights or from laws and regulations. Any change of the purpose of the Processing requires a new assessment on whether the Processing for the new purpose is compatible. The closer the new purpose is to the initial purpose, the higher is the likeliness that the Processing for the new purpose is also lawful and fair. The principle allows addressing, whether the Processing within new technologies involves significant high risks within the intended extended use in order to ensure that the extended use is done responsibly. The risks for the Individual can be reduced with measures like pseudonymization, limited data sets, conversion of Personal Data to or derivation of synthetic data from the Personal Data, which may allow the processing for the new purpose lawful. Any further processing for purposes in the public interest like scientific or historical research or statistics etc. are typically compatible with the initial purposes and, thus, lawful and fair. This typically includes scientific research in the health care domain.

4. DATA RELEVANCE

Text	Guidance / Commentary
Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.	The collection of the Personal Data shall be relevant to the legitimate purposes. Where emerging technologies are used it may be relevant and necessary for the respective purpose to collect more Personal Data in order to get more reliable, more efficient or results with a higher degree of automation. The risks, which are involved from such higher amount of Personal Data must be addressed and mitigated within the principle of data security.

5.DATA QUALITY

Text	Guidance / Commentary
Personal Data shall be accurate and – to the extent necessary for the purposes of use – complete and kept up-to date.	Processing Personal Data, including making decisions about the Individual, based on inaccurate, incomplete or out of date data, is not in the interest of the Individual. Data quality is a prerequisite for data driven business models including emerging technologies like AI.
The Individual shall have enforceable rights to get: • incorrect Personal Data corrected; • if adequate in the context of the purpose – incomplete or outdated Personal Data completed and/or kept up-to date; and • Personal Data deleted if the Controller has no legitimate ground to keep them.	Governments may define the pre-requisite, which must be fulfilled for the Individual to claim and enforce such rights.

6. TRANSPARENCY

Text	Guidance / Commentary
Personal Data shall be Processed in a transparent manner in relation to the Individual. Controllers shall provide clear, understandable and easily accessible statements about their practices and policies with respect to Personal Data that shall include at a minimum:	This Principle is directed towards ensuring that the Individual is able to know what data is collected about them and for what purpose it is to be used. By providing notice, Controllers enable the Individual to make an informed decision about interacting with the Controller. Depending on the context in which the Personal Data is collected, notice methods may vary. For example, a common method for Controller to inform the Individual is to post privacy notices on their websites. In direct communication settings, display, paper or oral notices may be used.
a) the fact that Personal Data is being collected;	This part of the principle links the transparency with the principle of choice as part of the fairness principle.
b) the purposes for which Personal Data is collected;	This part of the principle links the transparency with the principle of purpose limitation.
c) the types of persons or organizations to whom Personal Data might be disclosed; and	This part of the principle shall enable the Individual to track where their data is, including data which is transferred to Processors.
d) the identity and location of the Personal Data controller, including contact information;	This part of the principle shall allow the Individual to enquire about the processing of their data and enforce their rights as necessary.
unless to the extent the Individual must be already reasonably aware of such data, information proves impossible or would involve a disproportionate effort or providing the information is not allowed according to national laws or subject to professional confidentiality.	If third parties already have informed the Individual or if the information is already in the public domain, it may not be necessary to inform the Individual. For example, if an agent collects an application form with Personal Data from the Individual for the purpose of forwarding it to a company, which shall make a contractual offer on that basis, the Individual is reasonably aware of such company, the Personal Data it receives and the purposes. Thus, the company in this case does not have to give an information notice to the Individual. Also, if it is unclear and difficult to identify, which Individual is subject of the Personal Data, for example Internet usage data, the Controller may not have to notify the Individual due to disproportionate efforts.

	National laws may prohibit disclosing that Personal Data are processed, for example in investigations. In that case, also no information notice towards the Individual is required. Lastly, also Processing by lawyers or other professions, which are legally bound to confidentiality, taking place within their professional activity may – under certain circumstances – not require an information notice of the Individual, whose Personal Data are Processed, where it conflicts with the tasks assigned to their profession under applicable laws.
All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of Personal Data. Otherwise, such notice should be provided as soon after as is practicable.	As a general rule, Controllers shall inform the Individual at the time of, or before, data are collected about them. At the same time, there may be circumstances, in which it is not feasible to do so, e.g. if the Controller does not receive the Personal Data from the Individual directly. It the latter case, information notice shall be provided soon thereafter.
The Individual shall have enforceable rights to obtain access to their Personal Data held by Controllers. Access shall be granted within a reasonable time, in a reasonable manner and in a form that is sufficiently easily understandable.	Governments may define the pre-requisite, which must be fulfilled for the Individual to claim and enforce such rights.

7.STORAGE LIMITATION

Text	Guidance / Commentary
Personal Data shall be kept in a form, which permits identification of the Individual for no longer than is necessary for the purposes for which the Personal Data are Processed.	This principle acknowledges that Personal Data must be deleted once it is no longer necessary for the purpose. The Controller must ensure deletion.

8.DATA SECURITY

Text	Guidance / Commentary
Recognizing the interests of the Individual to legitimate expectations of privacy and protection of their data, the Processing of Personal Data shall be designed in a way to prevent the inappropriate use or misuse of such data acknowledging the risk that harm may result from such inappropriate use or misuse.	This principle is part of risk management, as especially applying to new technologies and High-Risk Processing. The principle also foresees data protection by design considerations. This means that already in the design phase there may be risks for the Individual foreseeable and therefore should be addressed already in this phase. This also concerns emerging technologies, where the design should consider and mitigate privacy risks and implications. Any such measure to be taken is subject to a proportionate test. As a result, Personal Data may need to be Pseudonymized.
Controllers and Processors shall protect Personal Data that they hold with appropriate safeguards against risks, such as loss or unauthorized access to Personal Data, or unauthorized destruction, use, modification or disclosure of data or other misuses. Such safeguards shall be proportional to the likelihood and severity of the potential harm, the sensitivity of the data and the context in which it is held and should be subject to periodic review and re-assessment as well as appropriate threat protection monitoring.	This principle addresses data security concepts like confidentiality and integrity. When using AI this may include ensuring robustness and being able to explain the results of the Processing.
Where there has been a significant security breach on Personal Data, there shall be measures to be taken by the Controller, Processor and/or authorities to mitigate the risks for the Individual.	When a significant security breach occurs, it may help to reduce the risk of harmful consequences to the Individual concerned by mandating authorities to be notified by Data Controllers and Processors of the breach.

9.ACCOUNTABILITY

Text	Guidance / Commentary
A Controller /Processor shall be accountable for complying with measures that give effect to the DCO Privacy Principles stated above.	Controllers and Processors are responsible for, and must be able to demonstrate, compliance with the DCO Privacy Principles.
The Controller shall document internally Processing including the related purposes. The documentation shall in particular include how risks from High-Risk Processing have been addressed.	The documentation also facilitates the Controller to manage and leverage existing data and data use.
Controllers and Processors shall adequately train their staff to enable them applying the DCO Privacy Principles in their respective tasks.	Training is an important element for an effective implementation of the DCO Privacy Principles.
Individuals shall have enforceable privacy rights towards the Controller and Processor.	This element foresees that the Individual can effectively take measures which ensure that the Processing of his or her Personal Data is actually in compliance with the DCO Privacy Principles as implemented by national laws.
Compliance with the DCO Privacy Principles is monitored and supervised by competent supervisory authorities.	The oversight on compliance lies with an independent data protection authority and/or any other authorities, which are responsible for the supervision of compliance with privacy provisions under national laws.

@dcorg | www.dco.org