Nestor Nestor Diculescu Kingston Petersen
ATTORNEYS & COUNSELORS

Legal & Tax

30 years anniversary

Check list for key elements defined by EDPB for data protection by design and by default

The key elements derive from para. 61, 63, 65, 67, 71, 77 and 80 of the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (accessed on 8 May 2020).

Key design and default elements		Recommended approach
1.	**For transparency**	
1.1.	Clarity	Information shall be in clear and plain language, concise and intelligible.
1.2.	Semantics	Communication shall have a clear meaning to the audience in question.
1.3.	Accessibility	Information shall be easily accessible for the data subject.
1.4.	Contextual	Information shall be provided at the relevant time and in the appropriate form.
1.5.	Relevance	Information shall be relevant and applicable to the specific data subject.
1.6.	Universal design	Information shall be accessible to all, include use of machine readable languages to facilitate and automate readability and clarity.
1.7.	Comprehensible	Data subjects shall have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.
1.8.	Multi-channel	Information should be provided in different channels and media, beyond the textual, to increase the probability for the information to effectively reach the data subject.

NNDKP CONTACT

For any data protection and privacy related questions, please contact Roxana Ionescu, Head of NNDKP's Data Protection practice.

Note: This document should not be copied, disclosed, distributed or reproduced, in whole or in part, without the prior written consent of Nestor Nestor Diculescu Kingston Petersen. The contents of this document is for information purposes only and should not be relied upon or construed as legal or other kind of advice.

2. For lawfulness

2.1.	Relevance	The correct legal basis shall be applied to the processing.
2.2.	Differentiation	The controller shall differentiate between the legal basis used for each processing activity.
2.3.	Specified purpose	The appropriate legal basis must be clearly connected to the specific purpose of processing.
2.4.	Necessary	Processing must be necessary for the purpose to be lawful. It is an objective test which involves an objective assessment of realistic alternatives of achieving the purpose.
2.5.	Autonomy	The data subject should be granted the highest degree of autonomy as possible with respect to control over personal data.
2.6.	Consent withdrawal	The processing shall facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, any given consent is not valid.
2.7.	Balancing of interests	Where legitimate interests is the legal basis, the controller must carry out an objectively weighted balancing of interests. There shall be measures and safeguards to mitigate the negative impact on the data subjects, and the controller should disclose their assessment of the balancing of interests.
2.8.	Predetermination	The legal basis shall be established before the processing takes place.
2.9.	Cessation	If the legal basis ceases to apply, the processing shall cease accordingly.
2.10.	Adjust	If there is a valid change of legal basis for the processing, the actual processing must be adjusted in accordance with the new legal basis.
2.11.	Default configurations	Processing must be limited to what the legal basis strictly gives grounds for.
2.12.	Allocation of responsibility	Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject.

3. For fairness

3.1.	Autonomy	Data subjects shall be granted the highest degree of autonomy possible with respect to control over their personal data.
3.2.	Interaction	Data subjects must be able to communicate and exercise their rights with the controller.
3.3.	Expectation	Processing should correspond with data subjects' expectations.
3.4.	Non-discrimination	The controller shall not discriminate against data subjects.
3.5.	Non-exploitation	The controller shall not exploit the needs or vulnerabilities of data subjects.
3.6.	Consumer choice	The controller should not "lock in" their users. Whenever a service or a good is personalized or proprietary, it may create a lock-in to the service or good. If it is difficult for the data subject to change controllers due to this, which may not be fair.
3.7.	Power balance	Asymmetric power balances shall be avoided or mitigated when possible. Controllers should not transfer the risks of the enterprise to the data subjects.
3.8.	Respect rights and freedoms	The controller must respect the fundamental rights and freedoms of data subjects and implement appropriate measures and safeguards to not violate these rights and freedoms.
3.9.	Ethical	The controller should see the processing's wider impact on individuals' rights and dignity.
3.10.	Truthful	The controller must act as they declare to do, provide account for what they do and not mislead the data subjects.
3.11.	Human intervention	The controller must incorporate qualified human intervention that is capable of recovering biases that machines may create in relation to the right to not be subject to automated individual decision making in Article 22.
3.12.	Fair algorithms	Information shall be provided to data subjects about processing of personal data based on algorithms that analyze or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements.

4. For purpose limitation

4.1.	Predetermination	The legitimate purposes must be determined before the design of the processing.
4.2.	Specificity	The purposes must be specific to the processing and make it explicitly clear why personal data is being processed.
4.3.	Purpose orientation	The purpose of processing should guide the design of the processing and set processing boundaries.
4.4.	Necessity	The purpose determines what personal data is necessary for the processing.
4.5.	Compatibility	Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
4.6.	Limit further processing	The controller should not connect datasets or perform any further processing for new incompatible purposes.
4.7.	Review	The controller must regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.
4.8.	Technical limitations of reuse	The controller should use technical measures, including hashing and cryptography, to limit the possibility of repurposing personal data.

5. For data minimization

5.1.	Data avoidance	Avoid processing personal data altogether when this is possible for the relevant purpose.
5.2.	Relevance	Personal data shall be relevant to the processing in question, and the controller shall be able to demonstrate this relevance.
5.3.	Necessity	Each personal data element shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.

5.4.	Limitation	Limit the amount of personal data collected to what is necessary for the purpose.
5.5.	Aggregation	Use aggregated data when possible.
5.6.	Pseudonymization	Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately.
5.7.	Anonymization and deletion	Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted.
5.8.	Data flow	The data flow shall be made efficient enough to not create more copies, or entry points for data collection than necessary.
5.9.	*"State of the art"*	The controller should apply available and suitable technologies for data avoidance and minimization.

6. For accuracy

6.1.	Storage criteria	Data sources should be reliable in terms of data accuracy.
6.2.	Degree of accuracy	Each personal data element shall be as accurate as necessary for the specified purposes.
6.3.	Measurably accurate	Reduce the number of false positives/negatives.
6.4.	Verification	Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing.
6.5.	Erasure/rectification	The controller must erase or rectify inaccurate data without delay.
6.6.	Accumulated errors	Controllers must mitigate the effect of an accumulated error in the processing chain.
6.7.	Access	Data subjects should be given an overview and easy access to personal data in order to control accuracy and rectify as needed.
6.8.	Continued accuracy	Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps.
6.9.	Up to date	Personal data shall be updated if necessary for the purpose.
6.10.	Data design	Use of technological and organisational design features to decrease inaccuracy, e.g. drop down lists with limited values, internal policies, and legal criteria.

7. For storage limitation

7.1.	Deletion	The controller must have clear internal procedures for deletion.
7.2.	Automation	Deletion of certain personal data should be automated.
7.3.	Storage criteria	The controller must determine what data and length of storage is necessary for the purpose.
7.4.	Enforcement of retention policies	The controller must enforce internal retention policies and conduct tests of whether the organization practices its policies.
7.5.	Effectiveness of anonymization/deletion	The controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data, and should test whether this is possible.
7.6.	Disclose rationale	The controller must be able to justify why the period of storage is necessary for the purpose, and disclose the rationale behind the retention period.
7.7.	Data flow	Controllers must beware of and seek to limit "*temporary*" storage of personal data.
7.8.	Backups/logs	Controllers must determine which personal data and length of storage is necessary for back-ups and logs.

8. For integrity and confidentiality

8.1.	Information security management system (ISMS)	Have an operative means of managing policies and procedures for information security. For some controllers, this may be possible with the help of an ISMS.
8.2.	Risk analysis	Assess the risks against the security of personal data and counter identified risks.
8.3.	Resilience	The processing should be robust enough to withstand changes, regulatory demands, incidents and cyber attacks.
8.4.	Access management	Only authorized personnel shall have access to the data necessary for their processing task.
8.5.	Secure transfers	Transfers shall be secured against unauthorized access and changes.
8.6.	Secure storage	Data storage shall be secure from unauthorized access and changes.
8.7.	Backups/logs	Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control.
8.8.	Special protection	Special categories of personal data should be protected with adequate measures and, when possible, be kept separated from the rest of the personal data.
8.9.	Pseudonymization	Personal data and back-ups/logs should be pseudonymized as a security measure to minimize risks of potential data breaches, for example using hashing or encryption.
8.10.	Security incident response management	Have in place routines and procedures to detect, handle, report and learn from data breaches.
8.11.	Personal data breach handling	Integrate management of notification (to the supervisory authority) and information (to data subjects) obligations in the event of a data breach into security incident management procedures.
8.12.	Maintenance and development	Regular review and test software to uncover vulnerabilities of the systems supporting the processing.