Rådet for
Digital Sikkerhed

Marts 2019[1]

Data Ethical Principles of the Danish Digital Security Council

- checklist for legislative proposals and distinct digital initiatives, etc.

To the Digital Security Council it is important that citizens can trust that their data is processed lawfully, fairly and ethically. Hence the Digital Security Council recommends that decision-makers, who propose new legislation, new digital solutions or want a given purpose fulfilled by digital means, review the list below and assess whether the action can be achieved within these ten principles:

1. **NECESSITY**
   Can the purpose be achieved completely without collecting personal data or by fully anonymising data?
   (if so, then choose this solution and disregard the checklist otherwise)
2. **LEGALITY**
   Is the proposal legal and in compliance with the law?
   (is the method legal due to consent, legitimate interests, contract or special law)
3. **ETHICAL DESIGN**
   Are the rights of the individual and the principles of the GDPR guaranteed through the design of the IT solution?
   (predetermined purpose, only collection of necessary data, insight, disclosure, control of own data, deletion, etc.)
4. **CONSEQUENCES**
   Has a prior decision been taken on the possible consequences of the proposal/solution for data subjects in the short and long term?
5. **FREEDOM OF CHOICE**
   May individuals freely choose whether or not data on them are recorded?
6. **SECURITY**
   Does the proposal build on an appropriate level of security in and around the system, that are in line with the necessary and best available technical and organisational methods?
7. **TRANSPARENCY**
   Does the proposal provide transparency in processing, including using algorithms, and is there human control over the fairness of results?
8. **RESPECT FOR HUMAN RIGHTS**
   Does the proposal guarantee that data processing is not biased with the risk of discrimination, marginalisation or stigmatisation of individuals?
9. **PROPORTIONALITY**
   Has a balance of proportionality been made to ensure that the rights of the individual are not undermined by a "the end justifies the means" way of thinking?
10. **RESPONSIBILITY**
    Are location of responsibilities, ongoing supervision, and official complaint access easily available?

[1] English translation from original Danish document (https://static1.squarespace.com/static/5592479ee4b0224fac5497af/t/5d00e6560187cc00011c703b/1560340055738/RfDS%2BDE-principper.pdf) by N. C. Juul, November 2020.

Rådet for
Digital Sikkerhed

Background

Personal data are an important source for developing digital services and fulfilling commercial, political and societal purposes. It is therefore relevant for companies, authorities and organisations alike to collect and process personal data.

It may be perfectly legitimate to wish to process personal data, but that does not change the fact that the processing has to be assessed against a number of legislative and ethical principles.

As follows from Section 72 of the Danish Constitution, the Universal Declaration of Human Rights Article 12, Article 8 of the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union Article 8, the individual has the right to privacy protection.

Even though this right might be superseded, the Digital Security Council (RfDS) considers that if the right is to be waived, it is important that this should be done on the basis of a thorough analysis which has assessed whether one can achieve its purpose in a less intrusive way.

The RFDS notes that proposals are being made periodically, the purpose of which may be noble, but in which no assessment has been made as to whether the same objective could be achieved with less intrusive means.

Examples include proposals for amending the Centre for Cyber Security Act, the so-called 'Gladsaxemodel', well-being studies in the school system and the case of the extension of diagnoses registered in the General Medical Database (DAMD).

There are a wide range of technological opportunities that are greatly overlooked in a political context when making proposals involving the processing of personal data. These include, among other things, anonymisation, pseudonymisation and multiparty computation (use of multiple identities).

The Council wants this type of technology to be used much more to support the right to privacy.

Data ethics principles for assessing new data initiatives

The RfDS has therefore clarified the principles that should be taken into account when new proposals are made or initiatives are taken to use new digital solutions. A number of these proposals already follow from the existing personal data law. It is essential that policy makers do not disregard these principles with their proposals.

To limit the number of suggestions that without necessity override the individual's right to privacy, the RfDS has created this checklist. Decision makers can use this checklist, when considering whether they achieve a given purpose without compromising the privacy of the individual – thus balancing the intent/objective optimally in terms of the means used.

The Digital Security Council therefore recommends that all 10 questions can be answered with a YES before a legislative or concrete IT solution is implemented.