A MATTER OF TRUST

Photo: David Cheshire/Loop Images/laif

Privacy and data security in development projects

Nowadays, the development context would be quite inconceivable without the collection and use of large sets of data. This also raises the question how such data should be handled and protected. Our author insists that the same standards have to apply in the North and in the South.

The right to privacy is a human right which was first enshrined in the Universal Declaration of Human Rights in 1946 and reiterated in the International UN Covenant on Civil and Political Rights in 1966. Privacy is therefore not merely a "first-world problem" (Kate McKee) although there are cultural differences of what people around the world consider to be private information. Furthermore, it is not just privacy that is at stake today in an increasingly digitised environment: since more and more personal data are collected in cities as well as in the rural context, the question is: who is in charge of these data collections, and does the individual citizen, consumer or farmer have any chance to learn about the processing of his data, let alone to control this processing? It would certainly be true to say that farmers in Africa have different and bigger problems than protecting their data. At the same time this statement is somewhat patronising in view of the guarantees on data protection which people in developed countries enjoy. Therefore, aid agencies based in Europe or e.g. Canada have to comply with the rules on data privacy and security of their respective countries when they are engaged in development projects in Africa and elsewhere. At the same time, manufacturers of agricultural technology should not be allowed to undercut data protection standards established in developed countries when selling their hard- and software to African farmers.

Alexander Dix
European Academy for Freedom of Information and Data Security
Berlin, Germany
dix@eaid-berlin.de

Data protection

Data protection (sometimes called "data privacy") goes beyond the concept of privacy because it gives the data subject rights to access and rectify his personal data and have them deleted once their storage is no longer necessary. More importantly, the developed and developing countries have agreed in the Organisation for Economic Co-operation and Development (OECD) framework on Guidelines for the Protection of Privacy and the Transborder Flows of Personal Data (1980, revised in 2013). These Guidelines demonstrate that governments consider economic co-operation and development – the right to an adequate standard of living is enshrined in the International Covenant on Economic, Social and Cultural Rights since 1966 – and data protection not to be contradictory but complementary values. This is particularly important in view of the fact that personal data are processed globally and services requiring the collection of such data are offered on a worldwide basis.

Why are privacy and data protection important in the development context? In many developed countries (e.g. in the European Union, North America, Australia, Japan) legal frameworks for data protection have been established with certain differences but with some main commonalities: personal data shall be collected in a transparent fashion, the data subject has a right to access these data and find out for what purposes they are used and how long they are stored by governments and industry. As far as the private sector is concerned personal data should only be collected with the informed consent of the data subject and only to the extent which is necessary for a specific purpose. In view of digitisation evolving at break-

neck speed, it is crucial that the data subject can trust that the data he discloses to make use of certain services or machines with data-processing capabilities are not used for different purposes (e.g. marketing). Data privacy is a key element to create this trust.

Three examples may illustrate this. Smart farming (or as it is also called: precision farming) requires the collection and use of large sets of data on the status of the soil, weather, resources, cultivation and management of the farm. These data are, in most cases, personal data of the farmer and only occasionally data referring to a co-operative (non-personal data). The farmer who uses equipment with the capacity to store these data will often want to process and analyse his "digital crops", i.e. the knowhow he has gained while engaging in smart farming. These "digital crops" are of economic value to him, and he may not want to share them with his competing neighbour. He may also think twice if a foreign company offers him the use of cloud-based services for smart farming because the farmer wants to be sure that he stays in control of these data. What happens if the company goes bust or is sold to another company which does not seem to be as trustworthy as the original service provider? Therefore the farmer may prefer to use hard- and software which allows for the local storage of his data.

Secondly, a company selling electronic farm machinery with data storage may not allow the farmer to extract the data if he wants to switch to machinery of another manufacturer. Europe is introducing the "right to data portability" in 2018, which would prevent this "lock-in" effect making farmers dependent on one particular technology or corporation and thereby preventing competition. This is at least just as important globally and in relation to developing countries, where foreign companies often dominate the markets.

Finally, access to financial resources (financial inclusion) is another area where privacy and data protection are increasingly seen as issues which need to be addressed in order to make sure that digital financial services do not have an exclusive instead of an inclusive effect on farmers and other persons applying for microcredits. The G 20 High Level Principles of 2016 therefore call for the establishment of responsible financial practices and a "sound consumer and data protection framework" which is "essential to building trust and confidence in the acquisition and on-going use of digital financial services, especially for consumers with limited financial literacy or the resources to absorb losses" (Principle 5). The G20 governments are continuing discussions on how to put flesh on this rather general statement. Obviously, financial institutions have a legitimate interest to check the financial status of potential customers as to their capacity to pay back credit and at the same time to protect from over-borrowing. However, this does not justify the excessive collection of personal data with no relevance to this purpose. Since persons in need of capital may agree even to illegitimate forms of data collection, consent is not a sufficient legal basis. What is needed is sensible regulatory restrictions on the collection of personal data at national and international level. The revised OECD Guidelines (2013) and the European Data Protection Regulation (2016) are possible blueprints here.

Data security

Data protection limits the collection and use of personal data. Data security is the other necessary component of informational autonomy: It requires the controller (i.e. the farmer or the provider offering the farmer services including the processing of personal data) to take the necessary technical and organisational measures to ensure the security and integrity of the processed data. This includes the protection of these data against unauthorised access by governments, hackers and identity thieves. The rise in the number of personal data breaches is staggering, as has become obvious in countries where the law prescribes security breach notifications in any case to the supervisory authorities and in certain cases to the data subjects. African farmers should not content themselves with lower standards of data security than farmers in Europe or in North America. Anyone should be offered state-of-the-art encryption tools for storing and transmitting their personal data at no extra cost. The European Union is embarking on a novel concept in this context by supporting the idea of certification and seals in their Data Protection Regulation. Products and services which are developed following the principle of privacy by design and by default should be certified and given a seal demonstrating to the user that the technology has been designed and manufactured according to the relevant legal standards. Such products and services will have a competitive advantage especially if they are to receive preferential treatment in development projects and public procurement. This does not exclude completely possible abuses or leaks when deploying this technology, but it may create the necessary trust-based architecture for using digital services and devices.

Conclusion

A crucial issue in many development projects is the question how to balance the human rights to privacy and data protection with the human right to an adequate standard of living. But it would be a mistake to assume that there is a trade-off between the two rights. Adequate living standards can be achieved while respecting farmers' privacy and ensuring that they can stay in control over their personal data. The OECD Member States generally agreed on this when they adopted the revised OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 2013. As Albert Schweitzer put it in his Nobel Lecture in 1954, "For any enterprise, trust is the capital without which no effective work can be carried out." He was speaking on the issue of peace at the time. But the same is true for development projects. Data protection and security are cornerstones for building trust.