# *Draft*

*Version 5 October 2016*

# **PRINCIPLES ON THE RIGHT TO INFORMATION AND PRIVACY**

***Principles on how to make public the information held by public bodies that relates to the performance of public functions so as to ensure full accountability of decision making and spending of public funds***

*Recognising* that the right of access to information and the right to privacy are both fundamental rights enshrined in international human rights treaties and many national constitutions;

*Recalling* that both the right to of access to information and privacy are not absolute rights and may be subject to certain limitations as established by law and as necessary in a democratic society;

*Bearing in mind* that the adequate protection of the private lives and right to privacy of private persons is essential in order for every individual to enjoy dignity and freedom;

*Given* that the importance of access to information and the opening of data held by public bodies in ensuring public participation in governance and in public debate, in delivering accountability of government, in defending human rights, in advancing the fight against corruption, and in promoting sustainable development;

*Recalling* that the right of access to information as established in international law includes both the reactive dimension of responding to requests and the proactive dimension of publishing information proactively, and hence incorporates obligations to open data as well as a right to request and access government data with only limited exceptions;

*Noting* that international human rights standards and comparative law and jurisprudence extend the right of access to information to private bodies performing public functions and/or operating with public funds and/or and other private bodies as determined by national legislators;

*Believing* that as a general principle personal data about private individuals should not be made public, and that when it is published in the public interest, any potential negative impacts should be minimized;

*Desirous* to ensure that information necessary for participation and accountability enters the public domain whilst ensuring appropriate protection of privacy and data protection;

*Considering* that in many instances the balance between privacy and transparency will need to be worked out on a case-by-case basis;

*Noting* that the legal framework in any country comprises the constitutions, laws, regulations, and jurisprudence, as well as international treaty commitments;

*Employing* the following definitions:

*Public official*: Shall include any individual with responsible for performing public tasks and/or with decision-making powers (and their advisors), who are elected, appointed or employed within the executive or legislative branches of power at national, sub-national, or supra-national levels; within private bodies performing public functions and/or operating with public funds at least to the extent that the data relates to those activities; and within public international organisations domiciled or operational in the country concerned.[[1]](#footnote-2)

*Public body*: Shall include all branches of the State (executive, legislative and judicial) and other public or governmental authorities, at whatever level – national, regional or local – are in a position to engage the responsibility of the state. It shall also include private persons or entities which perform public functions and/or operate with public funds and/or and other private bodies which play a role in public life as determined by national legislators.[[2]](#footnote-3)

*Private body*: Private bodies and individuals who for reasons of their activities, their receipt of public funds or subsidies, and who are deemed by the legislator or through clearly established regulations to play a public role or where there is an overriding public interest in transparency about their activities, shall also be subject to these principles, provided that the is clearly defined by the legislator and/or is clearly permitted by the national legal framework.

*Basic Personal Data*: This data may include, *inter alia*, the full name, professional affiliation, job title, appointments and sanctions processes (including administrative and penal sanctions), employment history, working or personal address, email address, telephone number, ID number, birth date and other identifying data, as determined by the legislator on a case-by-case basis and/or as permitted by the national legal framework for balancing access to information and protection of privacy.

*Sensitive Personal Data*: Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[[3]](#footnote-4)

We propose that these principles be incorporated into the legal frameworks governing the right of access to information and protection of privacy:

1. Fundamental Rights to Information and to Privacy

The legal framework shall recognise both the right of access to information and the right to privacy and shall develop comprehensive and adequate mechanisms for their enjoyment and protection.

This legal framework must clearly define the relationship between these two fundamental rights and should ensure that there are clear mechanisms permitting decisions to be taken, on a case-by-case basis, as to when information containing private data should be released into the public domain.

1. Public functions of Public Officials

Information that relates to the activity of public officials, and to persons performing public functions and/or spending public funds should generally be made available.

At a minimum, the names, job titles, and other relevant basic data about the functions and activities senior public officials should be made public.

The definition of “senior” public officials should include those at any level of government who have responsibility for decision making and/or the spending of public funds.

1. Basic data about public officials

The legal framework shall make clear that all public officials shall expect that basic data, including names, job titles and details of responsibilities and involvement in decision-making processes, shall be made public.

The legal framework shall establish that curriculum vitae, assets declarations, and declarations of conflict of interest of all public officials shall be made available.

The participation of all public officials in meetings, inside or outside government, and their participation in decision-making processes shall be deemed to be, *prima facie*, public information.

All those who fall under a legal requirement to make public personal data that relates to their professional activities, shall be clearly informed about these obligations in advance of taking up any position and shall be informed of their rights to object to the publication of particular data, as well as the mechanisms for doing so.

The application of exceptions to the publicity of basic personal data about public officials shall be limited to those cases where such transparency would (a) fall under one of the legitimate exceptions to the right of access to information as defined by international standards and/or (b) reveal sensitive personal data, a defined by international standards.

1. Spending of public funds by public officials

When public officials are engaged in the spending of public funds, basic data on those responsible for and/or directly implicated in the spending of such funds shall always made available.

This shall also include details of the names and job titles of those responsible for decisions related to the spending of public funds.

This shall also include the spending of public funds directly related to the public officials on salaries and other benefits, on travel expenses, on hospitality or entertainment allowances.

1. Private recipients of public funds

Individuals working for private legal entities and natural persons who are recipients of public funds in the forms of public procurement contracts, subsidies and grants, shall do so with an expectation that basic personal data will be made available along with data on the funds received and the activities for which those funds are provided.

All private persons who fall under a legal requirement to make public personal data, shall be clearly informed about these obligations in advance of taking up any position and shall be informed of their rights to object to the publication of particular data, as well as the mechanisms for doing so.

1. Private persons engaging in decision-making processes

Private persons engaging in decision-making processes, including by participating in meetings with public bodies and by contributing to public consultations, shall do so with an expectation that basic personal data may be made available.

This expectation of publicity shall apply in particular to individuals engaged in lobbying and/or associated with private interest groups (lobbyists and similar organised groups) in accordance with the International Standards on Lobbying Regulation.

1. Obligation to Anticipate Disclosure

Public bodies that are holders of data that may be subject to disclosure under these principles and according to the national legal framework shall take necessary steps to record, organise, store, and administer data in a way that anticipates and facilitates disclosure.

These measures shall include, *inter alia*, storing data in electronic formats so that personal data that is not subject to disclosure may be easily redacted and withheld from disclosure when making public the information either proactively or upon request.

1. Non-public data about private persons

Public bodies applying the legal framework for transparency and access to information, and implementing open data rules and policies, shall take every necessary measure to ensure that the private data of private persons that is not otherwise subject to transparency obligations, and in particular any sensitive personal data, is protected from disclosure.

These measures shall include protections so that when multiple data sets are released under open data policies, it is not possible to identify the personal data of private persons. The mechanism for this may include decisions on which data is released and/or clear restrictions on how data may be used.

1. Reuse of Data Sets containing Private Data

All recipients of personal data shall be given clear instructions on the legal framework for the reuse of the personal data received.

As a general principle, information obtained under access to information laws and/or via the proactive publication of information may be used to exercise the rights to freedom of expression and information as enshrined in international human rights treaties. In other words, information may be used to form and express opinions, and may be shared with others without limitations and without frontiers.

The legal framework shall establish limits on the reuse of information in ways that might result in the identification of sensitive personal information about private individuals.

In no case may limits be placed on the reuse of information for the exercise of the right to freedom of expression, be it by journalists, civil society, or members of the public, even where such use is made to criticise or to hold to account the activities of public bodies and/or identifiable individuals.

Similarly, the use of personal data obtained in accordance with these principles and as authorised by the national legal framework shall not be limited where that use is made in order to participate in public decision-making processes.

1. Independent Oversight

The national legal framework shall establish oversight mechanisms for ensuring an adequate balancing between the right of access to information and protection of privacy personal data in line with these principles and the national legal framework.

To the extent that they exist, this responsibility will fall with the Information Commissioner or Commission and the national Data Protection Agency, or their equivalents. In the case that both bodies exist and are not a combined entity, the legal framework shall establish clear mechanisms for co-decision making and oversight of the release of personal data in the public interest.

In all cases, the oversight body shall be independent of government, shall have a budget set by and shall report to parliament, shall have powers of investigation and sanction, and shall have sufficient resources adequately to carry out its oversight role.

The legal framework shall provide clear, rapid, and low-cost mechanisms for appeal, both to the oversight body and to the courts, for any individuals, inside or outside of public bodies who wish to raise concerns about the protection of their personal data. These mechanisms should also permit appeals for those who wish to challenge refusals to or failures to make public relevant personal data where there is a public interest in doing so.

***Version 3 – 5 October 2016***

***Access Info Europe and Shtiftung NV***

1. See UN General Comment No. 34, July 2011: <http://bangkok.ohchr.org/programme/documents/general-comment-34.aspx> [↑](#footnote-ref-2)
2. See General Comment No. 34 ibid and Council of Europe Convention on Access to Official Documents <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205> [↑](#footnote-ref-3)
3. Definition of sensitive data from the EU Data Protection Regulation: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> [↑](#footnote-ref-4)