Source code

Applicable to mass-market software or products containing such software (explicitly excluding software used for critical infrastructure), the source code rules, in their core, prohibit Members from requiring to transfer or grant access to source code of a software owned by a natural or juridical person from another Member, or an algorithm expressed in such source code ("Algorithm" means a defined sequence of steps [,] taken to solve a problem or obtain a result), as a condition for the import, distribution, sale, or use of that software, or of productscontaining that software, in its territory.

The essence of the source code rules is, however, in the exceptions applicable to them. Among those: voluntary transfer of source code under commercially negotiated contracts, as a part of a public procurement transaction, or under open-source license, such as in the context of open source coding; a requirement to modify the source code necessary for the software to comply with laws or regulations; requirement of source code transfer as a means of imposing ex-post regulation; general, security and prudential exceptions.

In addition, the draft also identifies the situations, in which the regulatory, conformity-assessment body or judicial authority would have to be granted access to the source code, namely, to preserve the source code or algorithm expressed therein for investigation, inspection, examination, enforcement action, monitoring of compliance with code of conduct or other standards, or judicial proceedings, subject to safeguards against unauthorized disclosure; for imposition or enforcement of a remedy granted following investigation, inspection, examination, enforcement action, or judicial proceedings; as required by a court, administrative tribunal, or by a competition authority to remedy a violation of competition law; for the protection and enforcement of intellectual property rights; to take action that is considered necessary for the protection of essential security interest relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defense purposes; as a part of patent application or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to non-disclosure safeguards.

ICT Products that use cryptography

The proposed rules addressing cryptography complement the source code disciplines discussed in 29 (NB: the source code disciplines are, however, distinguished from the cryptography rules).

The submissions build on several definitions: of “cipher” or “cryptographic algorithm” (a mathematical procedure or formula for combining a key with plaintext to create a ciphertext), “ciphertext” (data in a form that cannot be easily understood without subsequent decryption), “cryptography” (the principles, means or methods for the transformation of data in order to conceal or disguise its content, prevent its undetected modification, or prevent its unauthorised use; and is limited to the transformation of information using one or more secret parameters, for example, crypto variables, or associated key managemen), “encryption” (the conversion of data (plaintext) through the use of a cryptographic algorithm into a [ciphertext / form that cannot be easily understood without subsequent reconversion (ciphertext)] [and/using] the appropriate [cryptographic] key), “key” (a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that [an entity / a person] with knowledge of the key can reproduce or reverse the operation, while [an entity / a person] without knowledge of the key cannot) and “commercial ICT product” (means a product [, including digital products,] [that is designed for commercial applications and] whose intended function is information processing and communication by electronic means, including transmission and display, or electronic processing applied to determine or record physical phenomena, or to control physical processes), which is at the very core of the disciplines.

The main rules: With respect to an ICT product that uses cryptography and is designed for commercial applications, no Member shall require a manufacturer or supplier as a condition of the manufacture, sale, distribution, import or use to:

(a) transfer /provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification, or other design detail;
(b) partner or otherwise cooperate with a person in the territory of that Member in the development, manufacture, sale, distribution, import, or use of the [commercial] ICT product; or use or integrate a particular cryptographic algorithm or cipher.

Meanwhile, the disciplines do not apply to commercial ICT products which are financial instruments and their regulation; encryption controlled by the Member and required to be used by the enforcement authorities; requirement of a Member relating to access to networks, owned or controlled by the Member, including those of central banks; manufacture, sale, distribution or use of a commercial / ICT product by or for the Members; measures maintained pursuant to supervisory, investigatory, examination authority relating to financial services suppliers or financial markets.

In addition, regulatory and judicial authorities of a Member are not precluded from requiring a manufacturer or supplier of a commercial ICT product that uses cryptography:
(a) to preserve and make available any information for an investigation, inspection, examination, enforcement action or a judicial proceeding, subject to safeguards against unauthorised disclosure; or

(b) to transferor provide access to any information to which paragraph for the purpose of imposing or enforcing a remedy granted in accordance with that Member's competition law following an investigation, inspection, examination, enforcement action or a judicial proceeding.

Open internet access

The proposal is aimed at ensuring the user access to internet.
The alternative definitions of end-user and user both refer to natural person or enterprise, using or requesting to use the internet access service / available telecommunications service.
The main rules focus on enabling users on the Member's territory to access and use services and applications of consumer choice available on internet [regardless of the country where the service or application is being provided] subject to reasonable, non-discriminatory, proportional and transparent network management [compatible with the relevant international standards]; to connect devices of consumer choice to Internet (provided that such devices do not harm the network); and access transparent, clear, and sufficiently descriptive information on the network management practices of internet access service supplier. The above rules might be subject to Member's applicable policies, laws and regulations.

Open government data (JSI context)

The disciplines are put together following the recognition by the Members that facilitating public access to and use of [open] government data fosters economic and social development, competitiveness, and innovation

Definitions: [without prejudice to Member's IP laws] "Government data "means data, including metadata, (i) held by the central government and (ii) public disclosure of which is not restricted under domestic law. "Open governmental data" (data held by the central government, [and to the extent provided for in the laws and regulations of a [Party/Member], by other levels of government,] which is made available for public access and use, as determined by the [Party/Member].]) and "Metadata" (structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions) are also defined.

The main rule instructs the Members to endeavor to [identify] and [publish] open governmental data, facilitating public access and use of it, through expanding the coverage of open government data, allowing the public to request or recommend disclosure of particular data held by the government; ensuring that the relevant data is in a machine-readable / searchable / open format; that such data is [timely] updated; and properly documented using [commonly used] metadata schemes.

The text also suggests allowing a user of the governmental data to: use, reuse and redistribute it; regroup its components; modify or retrive information contained in the open government data; use it for commercial and non-commercial purposes (including a link to original sources, where possible).

Finally, the text concludes by the provisions encouraging cooperation and experience sharing in the area.