Cross-Border Data Forum

What is 'Data'?

Definitions in International Legal Instruments on Data Protection, Cross-Border Access to Data & Electronic Evidence

Authored by Karine Bannelier & Anaïs Trotry[*]

The Cross-Border Data Forum

The [Cross-Border Data Forum](https://www.crossborderdataforum.org) (CBDF) is a 501(c)(4) non-profit group that addresses international data transfer policy issues. It seeks to promote and achieve four key goals: to fulfil legitimate law enforcement requests for data relevant to the investigation of serious crimes; to protect and promote privacy and human rights as essential elements in new legal approaches; to provide a workable regime for the companies that hold data of interest to law enforcement; to safeguard the Internet by resisting calls to localize data and splinter the Internet. The CBDF has published on its website a series of studies and articles on cross-border access to data and international cooperation concerning electronic evidence sharing: https://www.crossborderdataforum.org.

As a result of its role as an observer to the UN Ad Hoc Committee to elaborate a UN Cybercrime Convention, and its desire to help clarify the debate on international cooperation and access to data, the CBDF proposes here an analysis on what constitutes data and the different categories of data that could be relevant for the convention.

Requests for a Definition of "Data" Categories During the UN Convention on Cybercrime Negotiations

During the debate at the UN Ad Hoc Committee, provisions in the convention dedicated to international cooperation were considered by many States to be the most important provisions in the convention along with criminalization. In this regard, a number of questions concerning international cooperation revolved around the issues of electronic evidence sharing, transborder access to data and the protection of personal data. For instance, at the third session, the UN Ad Hoc Committee asked States the following question: "How should the chapter on international cooperation determine the requirements for the

---

[*] Karine Bannelier, Associate Professor in International Law, Director CyberSecurity Institute (University Grenoble Alpes) & Senior Fellow on Cybercrime at the Cross Border Data Forum. Anaïs Trotry, Phd Candidate, Chair Legal and Regulatory Implication of Artificial Intelligence (University Grenoble Alpes).

protection of personal data for the purposes of the convention?". While some States underlined the sensitivity of this question, the lack of a common understanding of the different categories of data that could be relevant for the convention and of a definition of "personal data" soon became evident. This situation led some States to ask for agreed definitions on what is meant by data, personal data/non-personal data, content data/non-content data, metadata, subscriber data, traffic data and sensitive data.

Absence of a Definition of Data in the UNTOC and UNCAC

The two UN conventions used as models by the UN Ad Hoc Committee, the UNCAC and the UNTOC, do not provide any definition of data and personal data. The UNTOC does not mention data at all, while the UNCAC mentions the protection of 'personal data' (art. 10) but does not define it.

Solutions Provided by Other International Instruments

Some stakeholders took the view that it is essential to keep in mind the evolution of the legal framework surrounding the protection of personal data, which has taken place in many States since the negotiation of the UNTOC and UNCAC conventions, and to include provisions according to which State parties remain free to make cooperation dependent on the recipient ensuring appropriate data protection safeguards. Other States claimed that it would be useful to rely on the solutions provided by the Budapest Convention or other regional instruments such as the African Union Convention on Cybersecurity and Data Protection.

Purpose of the Charts and Methodology

In order to aid the debate on this issue, we have identified, without being exhaustive, the most relevant and important international instruments[1] that provide definitions of the different categories of "data". We have examined instruments adopted by several international organizations, located on every continent, as well as bilateral instruments such as Mutual Legal Assistance Treaties which, generally, do not include any definitions of "data", and bilateral agreements on cooperation and exchange of information in the field of law enforcement.

Based on this analysis we have selected definitions that appear in 21 international instruments. Most of these instruments are binding international texts (international treaties, executive agreements, binding acts of international organizations such as EU regulations and directives), but we have also included certain important soft law instruments (from the OECD, the APEC etc.), as well as some texts that have not yet been adopted (such as the EU draft E-Evidence regulation[2] or the European Commission's proposal for an ePrivacy Regulation[3]) because of their importance.

The results of our analysis are presented in two charts. Chart 1 presents how the definitions of the different categories of data variously appear in these 21 international instruments. It also provides details and links for each instrument. Chart 2 compiles the full text of all the relevant definitions, under 3 major headings: 1) "Data – Generic Terms"; 2) "Non-personal data"; 3) "Personal Data" with all their subcategories: Subscriber Data; Metadata (Traffic Data; Location Data; Access Data; Transactional Data); Content Data; Sensitive Data (Health Data; Biometric Data; Genetic Data).

Main Findings and Outstanding Issues

The main findings of this comparative analysis are as follows:

- There is an international consensus about the definition of "personal data". According to this definition personal data means any information relating to an identified or identifiable natural person by which this person can be identified. This clearly shows, for instance, that information concerning a "legal" (such as a company or a public authority) rather than a "natural" person is not personal data, unless this legal person's data includes information which reveals the identity of a person (for instance, a specific name and a corporate email address relating to a particular individual, therefore constituting personal data).

- Beyond this consensus, nonetheless, several issues around interpretation remain. This has compelled international bodies, such as the "Article 29 Working Party", the European Data Protection Board's predecessor, which unites all European Data Protection Authorities, to issue guidance on how the four constituent elements in the definition of "personal data" found in EU instruments, namely 'any information', 'relating to', 'an identified or identifiable', and 'natural person'—ought to be interpreted.[4]

- In the field of electronic evidence, regional instruments and bilateral agreements often refer to three main categories of data of interest to law enforcement agencies: subscriber information; traffic/access and transactional data; and content data. These three categories correspond to different legal regimes and thresholds of procedural and substantive protections. The category of "subscriber information" benefits from fewer protections, while the two other categories, considered to be much more intrusive in terms of privacy and human rights, benefit from much greater protections in international instruments. However, researchers have noted that there can be significant spillover across these three categories, and also that the emergence of new services and data types, as well as other factors, might lead to a "re-evaluation of the notion of intrusiveness" and raise questions about whether the existing procedures linked to the categories of data are able to ensure that there are adequate protections and sufficient checks and balances.[5]

- Some personal data (including, but not limited to, biometric, genetic and health data) are considered to be particularly "sensitive", which has led to the creation of "special categories of data" with a corresponding special legal regime. In general, international instruments prohibit in principle the processing of such categories of data, subject to a series of exceptions.

- The delineation between personal data and non-personal data is of paramount importance in determining the scope of application of several data protection instruments. The category of "non-personal data" is generally defined in a negative way, as including all data which are not "personal". However, the way in which this is defined does not resolve all of the issues involved. The distinction between "personal" and "non-personal" data can be tricky sometimes, especially when personal and non personal data is mixed together in one dataset or in the context of personal data that have been anonymized, when there is a risk of re-identification.

PS. The Authors will welcome comments concerning any eventual mistakes inadvertently in the charts or suggestions concerning definitions found in additional international instruments that may be relevant. Please contact as at: karine.bannelier[at]univ-grenoble-alpes.fr.

---

[1] Our analysis only covers international instruments that reflect agreement between States about these definitions. We have not included definitions of data categories found in domestic laws.

[2] The EU E-Evidence regulation should be adopted in the coming months. Our Charts refer to the draft initially proposed by the European Commission ("EU E-Evidence Reg. Proposal") in 2018 as well as the draft adopted by the European Parliament in 2020 ("EU E-Evidence Parl. Draft").

[3] In 2017 the European Commission proposed the adoption of a Regulation concerning the respect for private life and the protection of personal data in electronic communications ("EU ePrivacy Reg. Proposal") as an alternative to the 2022 ePrivacy Directive. However, this regulation has not yet been adopted and the ePrivacy Directive remains in force.

[4] See Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data (WP 136) 01248/07/EN, 6.

[5] See Internet and Jurisdiction, "Framing Brief: Categories of Electronic Evidence", May 31, 2022.

WHAT IS 'DATA'? DEFINITIONS IN INTERNATIONAL LEGAL INSTRUMENTS

(Chart 1)

INSTRUMENTS	Computer Data [Computerized Data]	Electronic Evidence/Information/Communication Data	NON PERSONAL DATA	PERSONAL DATA	Subscriber Data/Information	Metadata	Traffic Data	Location Data	Access Data	Transactional Data	Content Data	Sensitive Data ('Special categories of personal data')	Health Data	Biometric Data	Genetic Data
AU Malabo Conv.	✓			✓								✓	✓		
APEC Privacy Fram.				✓											
ASEAN MCCs				✓											
COE Budapest Conv.	✓				✓		✓								
COE Prot. II Budapest Conv.				✓								✓			
COE Conv. 108 &108 +				✓								✓		✓	✓
Ibero Standards				✓								✓			
EU GDPR				✓								✓	✓	✓	✓
EU LED				✓								✓	✓	✓	✓
EU ePrivacy Dir.							✓	✓							
EU ePrivacy Reg. Proposal		✓				✓					✓				
EU Data Governance Act	✓		✓												
EU AI Act. Proposal														✓	
EU E-Evidence Reg. Proposal		✓			✓				✓	✓	✓				
EU E-Evidence Parl. Draft		✓			✓		✓				✓				
EU Free Flow Non-Personal Data Reg.			✓												
OECD Priv. Guid.				✓											
EU-US Umbrella Agr.				✓								✓			
Cloud Act Agrs.				✓	✓										

WHAT IS 'DATA'? DEFINITIONS IN INTERNATIONAL LEGAL INSTRUMENTS

- **AU Malabo Conv.** African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), African Union, 2012, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

- **APEC Privacy Fram.** APEC Privacy Framework, 2015, https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1

- **ASEAN MCCs.** ASEAN Model Contractual Clauses for Cross Border Data Flows, 2021, https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

- **COE Budapest Conv.** Convention on Cybercrime (Budapest Convention), Council of Europe, European Treaty Series — No. 185, 2001, https://rm.coe.int/1680081561

- **COE Prot. II Budapest Conv.** Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Council of Europe Treaty Series — No. 224, 12 May 2022, https://rm.coe.int/1680a49dab

- **COE Conv. 108 & 108+.** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Council of Europe, European Treaty Series-N°. 108, Strasbourg, 28.01.1981, https://rm.coe.int/1680078b37; Convention for the protection of individuals with regard to the processing of personal data (Convention 108 +), June 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

- **Ibero Standards.** Standards for Personal Data, Protection for Ibero-American States, 20 June 2017. https://www.dataguidance.com/sites/default/files/02.24.20_ibero-am_standards.pdf

- **EU GDPR.** Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FR

- **EU LED** Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 27 April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

- **EU ePrivacy Dir.** Directive on privacy and electronic communications : Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=FR

- **EU ePrivacy Reg. Proposal.** Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM (2017) 10 final, 2017/0003 (COD), Brussels, (proposed by the European Commission on 10 January 2017, not yet adopted). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=FR

- **EU Data Governance Act.** Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), 30 May 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

- **EU AI Act Proposal.** Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 2021/0106 (COD), Brussels, (proposed by the European Commission on 21 April 2021, not yet adopted). https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

- **EU E-Evidence Reg.Proposal.** Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final (proposed by the European Commission on 17 April 2018, not yet adopted). https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF

- **EU E-Evidence Parl. Draft.** Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Birgit Sippel, COM (2018)0225, (draft of the European Parliament, 11 December 2020). https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html

- **EU Free Flow Non-Personal Data Reg.** Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, 14 November 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN

- **OECD Priv. Guid.** OECD Privacy Guidelines Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

- **EU-US Umbrella Agr.** Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences ("Umbrella Agreement"), 2 December 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&rid=3

- **Cloud Act Agrs.** Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, 3 October 2019; https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern; Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, 15 December 2021. https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-and-australia

WHAT IS 'DATA'? DEFINITIONS IN INTERNATIONAL LEGAL INSTRUMENTS
(Chart 2)

1. DATA (Generic Terms)

1.1 Computer Data/Computerized Data

AU Malabo Conv.	COE Budapest Conv.	EU Data Governance Act
Computerized data means any representation of facts, information or concepts in a form suitable for processing in a computer system (art. 1)	Computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (art. 1)	Data means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording (art. 2)

1.2 Electronic Evidence/Information/Communication Data

EU E-Evidence. Proposal Reg.	EU E-Evidence Parl. Draft	EU ePrivacy Reg. Proposal
Electronic evidence means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data (art. 2)	Electronic information means subscriber data, traffic data, or content data lawfully stored by a service provider at the time of the issuing of a European Production or Preservation order, that is requested for the purpose of serving as evidence during the investigation, prosecution and court proceedings relating to a criminal offence in a Member State, in accordance with national law (art.2)	Electronic communications data means electronic communications content and electronic communications metadata (art. 4)

2. NON-PERSONAL DATA

EU Data Governance Act	EU Regulation Free Flow Non-Personal Data
Non-personal data means data other than personal data (art. 2)	Data means data others than personal data as defined in point (1) of Article 4 of the Regulation (EU) 2016/679 (art. 3). Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines. If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data (Recital 9)

3. PERSONAL DATA

3.1 Personal Data/Personal Information

AU Malabo Conv.	APEC Privacy Fram.	ASEAN MCCs	COE Prot. II Budapest Conv.	COE Conv. 108 & 108+	Ibero Standards	EU GDPR	EU LED	OECD	EU-US Umbrella Agr.	Cloud Act Agrs.
Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (art. 1)	Personal information means any information about an identified or identifiable individual (9) The Framework is intended to apply to information about natural living persons, not legal persons. The Framework applies to personal information, which is information that can be used to identify an individual. It also includes information that would not meet this criteria alone, but when put together with other information would identify an individual. For example, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behavior, social relationships, private preferences and identity (9. Commentary)	Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject") transferred under this contract (1.7)	Personal data means information relating to an identified or identifiable natural person (art. 3)	Any information relating to an identified or identifiable individual ("data subject") (conv. 108 & 108+ art. 2)	Any information regarding an individual identified or identifiable, expressed in a numerical, alphabetical, graphical, photographic, alpha-numeric, acoustic way, or of any other kind. It is considered that a person is identifiable when his identity can be determined directly or indirectly, provided that this does not require disproportionate deadlines or activities (art.2)	Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (art.4)	Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (art. 3)	Personal data means any information relating to an identified or identifiable individual (data subject). (par. 1)	Personal information means information relating to an identified or identifiable natural person. An identifiable person is a person who can be identified, directly or indirectly, by reference to, in particular, an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (art. 2)	Personal Data means information relating to an identified or identifiable individual (art. 1.12) (2021).

3.2 Subscriber Data/ Subscriber Information

COE Budapest Conv.	EU E-Evidence Proposal Reg.	EU E-Evidence Parl. Draft	Cloud Act Agrs.
Subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a) the type of communication service used, the technical provisions taken thereto and the period of service; b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c) any other information on the site of the installation of communication equipment, available on the basis of the service (art. 18)	Subscriber data means any data pertaining to: (a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email; (b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user (art. 2)	Subscriber data means any data, collected in the normal course of business, pertaining to the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or email address identifying the subscriber or customer as well as the type of service provided and the duration of the contract with the service provider, which is strictly necessary for the sole purpose of identifying the user of the service (art.2)	Subscriber information means information that identifies a subscriber or customer of a Covered Provider, including name, address, length and type of service, subscriber number or identity (including assigned network address and device identifiers) telephone connection records, records of session times and durations, and means of payment. (art. 1.16) (2021)

3.3 Metadata

EU ePrivacy Reg. Proposal

Electronic communications metadata means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication (art. 4)

3.3.1 Traffic Data

COE Budapest Conv.	EU eprivacy Dir.	EU E-Evidence Parl. Draft
Traffic data means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service (art. 1)	Traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof (art.2)	Traffic data means data collected in the normal course of business related to : (a) the type of service provided and its duration where it concerns technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of the service, excluding passwords or other authentication means used instead of a password that are provided by a user, or created at the request of a user; (b) the commencement and termination of a user access session to a service, such as the date and time of use, or the log-in to, and log-off from the service; (c) electronic communications metadata as processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content, including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment processed in the context of providing electronic communications services, and the date, time, duration and the type of communication (art.1)

3.3.2 Location Data

EU eprivacy Dir.

Location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (art.2)

3.3.3 Access Data

EU E-Evidence Proposal Reg.

Access data means data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications] (art.2)

3.3.4 Transactional Data

EU E-Evidence Proposal Reg.

Transactional data means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications] (art.2)

3.4 Content Data

EU E-Evidence Proposal Reg.	EU E-Evidence. Parl. Draft	EU ePrivacy Reg. Proposal
Content data means any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data (art.2)	Content data means the stored data in a digital format by the service provider such as text, voice, videos, images, and sound other than subscriber or traffic data (art.2)	Electronic communications content means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound (art.4)

3.5 Sensitive Data (Special Categories of Personal Information)

AU Malabo Conv.	COE Prot. II Budapest Conv.	COE Conv. 108 & 108 +	Ibero Standards	EU GDPR	EU LED	EU-US Umbrella Agr.
Sensitive data means all personal data relating to religious, philosophical, political and trade-union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions (art. 1)	Processing by a Party of personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, or trade union membership; genetic data; biometric data considered sensitive in view of the risks involved; or personal data concerning health or sexual life; shall only take place under appropriate safeguards to guard against the risk of unwarranted prejudicial impact from the use of such data, in particular against unlawful discrimination (art. 14)	Genetic data; – personal data relating to offences, criminal proceedings and convictions, and related security measures; – biometric data uniquely identifying a person; – personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, (Conv. 108+ art. 6) Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, (Conv. 108 art. 6)	Those that refer to the intimate sphere of their holder, or which undue use may originate discrimination or involve a serious risk thereto. In an illustrative way, personal data that may reveal aspects such as racial or ethnic origin; beliefs or religious, philosophical and moral convictions; union affiliation; political opinions; information regarding health, life, sexual preference or orientations, generic data or biometric data aimed at identifying the person in an unequivocal way (art.2)	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (art. 9.1)	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (art. 10)	Personal information revealing racial or ethnic origin, political opinions or religious or other beliefs, trade union membership or personal information concerning health or sexual life (art. 13)

3.5.1 Health Data

AU Malabo Conv.	EU GDPR	EU LED
Health data means all information relating to the physical or mental state of the data subject, including the aforementioned genetic data (art. 1)	Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status (art.4)	Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status (art. 3)

3.5.2 Biometric Data

COE Conv. 108 & 108 +	EU GDPR	EU LED	EU AI Act. Proposal
Biometric data uniquely identifying a person (Conv. 108+ art. 6)	Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (art. 4 (14))	Biometric data means personal data resulting from specific technical processing relating to the physical, physio¬ logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (art.3)	Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (art. 3)

3.5.3 Genetic Data

COE Conv. 108 & 108 +	EU GDPR	EU LED
Genetic data; – personal data relating to offences, criminal proceedings and convictions, and related security measures (Conv. 108+ art. 6)	Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question (art. 4 (13))	Genetic data means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question (art.3)