from 45 organisations in the healthcare sector – and approved by the Dutch Data Protection Authority provides regulations related to data processing principles, the definition of scientific research and best practices for carrying out data protection impact assessments.[175]

The Code of Conduct Health research provides extensive guidelines on data protection issues. It provides of a normative part with practical examples and decision trees and a substantiating party where every aspect of the code of conduct is further substantiated in detail.[176]

21 Poland

Maria Owczarek

21.1 Informed consent

21.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law…)	Brief description and scope
General Data Protection Regulation (GDPR).	https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en (English version)	Regulation (EU) 2016/679 of the European Parliament and of the Council	In Poland the main regulatory tool addressing data protection issues and informed consent is the GDPR.
The Constitution of the Republic of Poland of 2nd April 1997	The Constitution of the Republic of Poland (English version)	Hard law - the supreme legal act of the Republic of Poland	The supreme legal act of the Republic of Poland, enacted on 2 April 1997 by the National Assembly. The Constitution of the Republic of Poland establishes guarantees concerning the right to privacy and protection of personal data (Articles 47 and 51).
The Act of 10 May 2018 on the Protection of Personal Data (In	The Act of 10 May 2018 on the Protection	Hard law	The Act of 10 May 2018 on the Protection of Personal Data is a Polish law, adopted

[175] https://www.federa.org/sites/default/files/images/abcd-studie_verkorte_data_privacy_impact_analyse_dpia_15-06-2018.pdf

[176] https://www.federa.org/sites/default/files/bijlagen/coreon/gedragscode_gezondheidsonderzoek.pdf

Polish: Ustawa o Ochronie Danych Osobowych)	of Personal Data (English version)		by the Polish Parliament, regulating legal issues related to the protection of personal data, in particular ensuring the application of the provisions of the General Data Protection Regulation (GDPR). The Act sets forth: 1) the public entities obliged to designate a data protection officer and the mode of notifying about his or her designation; 2) the conditions and mode of accrediting the entity authorized to perform certification with regard to personal data protection, accredited by the Polish Centre for Accreditation, hereinafter referred to as "certification body", body monitoring a code of conduct and certification; 3) the mode of approving the code of conduct; 4) the authority competent in matters of personal data protection; 5) the procedure in case of an infringement of personal data protection provisions; 6) the mode of European administrative cooperation; 7) inspection of compliance with personal data protection provisions; 8) the civil liability for the infringement of personal data protection provisions and proceedings before court; 9) the penal liability and administrative fines for the

			infringement of personal data protection provisions The Act however does not introduce any specific provisions regarding informed consent.
Act of 21 February 2019 on amending certain acts in connection with ensuring the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)	https://uodo.gov.pl/pl/395/967 (Polish version)		This comprehensive legal act, known as "the Sectoral Act", amends 162 Acts in order to harmonise Polish legislation with regulations arising from the GDPR.
Act of 14 December 2018 on the protection of personal data processed in connection with preventing and combating crime	https://uodo.gov.pl/pl/395/896 (Polish version)		The act implements into Polish legal framework the Directive (EU) 2016/680
Wet basisregistratie personen (BRP)	https://wetten.overheid.nl/BWBR0033715/2019-02-03	Hard law	Regulates the processing of personal data in the National Persons Registry
Wet op de geneeskundige behandelingsovereenkomst (WGBO)	https://wetten.overheid.nl/BWBR0005290/2012-06-13#Boek7_Titeldeel7_Afdeling5	Hard law	Privacy and data protection regulation in the context of medical treatment agreements
Wet gebruik burgerservicenummer in de zorg	https://wetten.overheid.nl/BWBR00238	Hard law	Regulates the use of national ID-numbers in the healthcare sector

	64/2019-07-01		
NEN 7510	https://www.nen.nl/NEN-Shop/Norm/NEN-751012017-nl.htm	Standard	Dutch Data Protection Authority demand this standard as mandatory for medical service providers that process national ID-numbers
Rules of the Authority for Consumer Markets (ACM)	https://www.acm.nl/nl/onderwerpen/verkoop-aan-consumenten/verkopen-aan-consumenten/diensten-aanbieden	Soft law (however enforced by ACM on sanction of fines)	Rules around consumer sales, viz (however not exhaustive) mandatory information distribution, consumer consent, telemarketing restrictions, terms of service, terms and conditions etcetera
Rules of the Data Protection Authority (AP)	https://autoriteitpersoonsgegevens.nl/nl	Soft law (however enforced by AP on sanction of fines)	Rules around privacy and data protection. Website provides the 'translation' of the relevant privacy and data protection legislation and their applicability into daily practice.

Main regulatory tools addressing data protection issues and informed consent in Poland

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

No, there are no such provisions under the Polish law regulating processing of personal data by a natural person in the course of a purely personal or household activity.

(ii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

Yes, the regulation covering the national security in terms of data protection issues is the Act of 14 December 2018 on the protection of personal data processed in connection with preventing and combating crime, implementing into Polish legal framework the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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.

The Act is available on the Personal Data Protection Office's website: https://uodo.gov.pl/pl/395/896 (only in Polish version).

Name of Authority	Link (English version if possible be)	Is this an independent body?	Number of employees	Level of activity (according to your appreciation)?	Response to requirements, questions, etc. made by the public
Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/en (English version)	Yes, the Personal Data Protection Office is an independent body, based on Article 51 of the GDPR.	The total number of staff (FTEs) at the end of 2020 employed by the Personal Data Protection Office was 272.	According to my appreciation, the level of activity of the Polish Supervisory Authority – the Personal Data Protection Office (further referred also as: "the Polish SA") is high – both in terms of national activity (see the next column), as well as international cooperation (the Polish Supervisory Authority actively participates, inter alia, in the work of the European Data Protection Board, taking part in its expert subgroups).	The Polish SA undertakes activities aimed at eliminating inconsistencies occurring in sectoral law, e.g. preparing information and education materials, or sending requests for consideration of relevant amendments to the law. The Polish SA organises a number of training sessions for sectors and data protection officers. Currently the Polish SA is working on submitted applications for approval of the codes of conducts (the list of application is available(in Polish) here: https://uodo.gov.pl/pl/426/1109.

					Since 2009, the Polish SA has been running a nationwide educational programme "Your Data – Your Concern. Effective protection of personal data which is an educational activity addressed to students and teachers (more on the Polish SA's website: https://uodo.gov.pl/en/506). On the Polish SA's website (running both in Polish and English) President of the Office publics its positions on current issues requiring data protection guidance, such as: guidance on data processing by an employer in relation to remote working (inter alia: https://uodo.gov.pl/en/553/1134, https://uodo.gov.pl/en/553/1136) or by a school in relation to remote teaching (e.g. https://uodo.gov.pl/en/553/1249, https://uodo.gov.pl/en/553/1118) during the COVID-19

					pandemic). The Personal Data Protection Office maintains a Twitter account (both in Polish and English) and publishes a monthly newsletter for data protection officers containing guidance for DPOs (archived issues available, in Polish, here: https://uodo.gov.pl/pl/p/archiwum-newslettera-dla-iod).

Information regarding Data Protection Authorities, Poland

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

The Polish Act of 10 May 2018 on the Protection of Personal Data does not introduce any specific definition of "data processing for research purposes" or "research in public interest".

(iv) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

Yes, such specific safeguards were introduced by the Act of 21 February 2019 on amending certain acts in connection with ensuring the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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). Such safeguards have been introduced by the abovementioned Act e.g. in the Act of 28 April 2011 on the information system in health care.

(v) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

The Polish Act of 10 May 2018 on the Protection of Personal Data does not introduce any specific safeguards for processing sensitive data beyond article 9 of the GDPR.

However, other specific legislation contains additional safeguards or exemptions for the processing of sensitive data.

An example may be the Polish Labour Code that establishes in Art. 221b some specific rules with regard to processing sensitive data of the employee (see the provision below)[177].

"Art. 221b

§ 1. The consent of an applicant for employment or an employee may constitute the basis for the employer's processing of personal data referred to in Article 9(1) of the Regulation 2016/679 only if the providing of such personal data occurs on the initiative of the applicant for employment or employee. The provision of Article 221a § 2 shall apply accordingly.

§ 2. The processing of biometric data of an employee shall also be allowed where the provision of such data is necessary in order to control access to particularly sensitive information, the disclosure of which could cause damage to the employer, or access to sensitive premises.

§ 3. The personal data referred to in § 1 may be processed only by persons who have a written authorisation to process such data issued by the employer. The persons authorised to process such data are obliged to keep them secret."

Article 9(2)(h) of the GDPR refers to paragraph 3 which sets out additional requirements for the obligation of professional secrecy when processing special categories of data on the basis of this ground. Such obligation should be imposed by law and concern the data processors. In Poland, such provisions are among others those imposing the obligation to maintain professional secrecy of medical professions (e.g. medical secrecy), indicated in several provisions of the Polish law.

Another example of such a provision is Article 37 of the Act on Insurance and Reinsurance Activity, according to which the insurance company may require the insured or the person for whose account the insurance contract is to be concluded to undergo medical examinations or diagnostic tests with minimal risk, excluding genetic tests, in order to assess the insurance risk, determine the right to a benefit and the amount of this benefit.

(vi) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

Such Code of Conduct has not been approved in Poland yet. However, work is in progress to approve the codes of conduct concerning data processing in research, which are:

1. Code of conduct concerning the processing of personal data by private research agencies submitted by the Organisation of Public Opinion and Market Research Companies http://rodowbranzybadawczej.pl/.

2. Code of conduct for the health sector on healthcare providers and processors submitted by the Polish Federation of Hospitals http://rodowzdrowiu.pl/index.php/english/

[177] Please note that the examples mentioned above do not constitute an exhaustive list of the provisions containing additional safeguards for the processing of sensitive data in Poland.

3. Code of conduct for the processing of personal data in small medical establishments, submitted by the Federation of Health Care Employers' associations (Zielonogórskie agreement) https://www.federacja-pz.pl/index.php?mnu=wiadomosc&id=478.

(vii) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

No, Polish Act of 10 May 2018 on the Protection of Personal Data does not give any specific definitions of data processing for "statistical purposes".

(viii) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

Yes, please find below specific rules established in the Polish Act of 10 May 2018 on the Protection of Personal Data in relation (the Act on the Protection of Personal Data) to research institutes.

The Act on the Protection of Personal Data sets forth rules concerning the public entities obliged to designate a data protection officer and the mode of notifying about his or her designation.

According to Article 9 „The public authorities and bodies obliged to designate the officer referred to in Article 37 para. 1(a) of the Regulation 2016/679 shall mean: 1) entities of the public finance sector; 2) research institutes; 3) the National Bank of Poland".

According to Article 73(2) of the Act on the Protection of Personal Data "Entities of the public finance sector, research institutes and the National Bank of Poland, with respect to which the President of the Office issued a legally binding decision ascertaining an infringement, shall immediately publish on their websites or the Office's website in the Public Information Bulletin information about measures undertaken to execute the decision."

Moreover, in accordance with Article 102 (1) of The Act on the Protection of Personal Data „The President of the Office may, by way of a decision, impose administrative fines in the amount of up to PLN 100,000.00 on:

1) entities of the public finance sector referred to in Article 9 (1-12) and 14 of the Act of 27 August 2009 on Public Finance;

2) research institute,

3) the National Bank of Poland.

(…)

3. The administrative fines referred to in para. 1 and 2 shall be imposed by the President of the Office on the basis of and on terms and conditions stipulated in Article 83 of the Regulation 2016/679.".

21.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

No, the Act on the Protection of Personal Data does not introduce any additional rules concerning the data subjects, as such. However, the Polish legislator introduced, under

Article 23 of the GDPR, restrictions of the scope of obligations and rights provided for in Articles 12 to 22 (please see the answer below.

(ii) Are there any special requirements regarding informed consent at the national level?

No, there are no special requirements regarding informed consent at the national level.

(iii) Are there any special requirements regarding data processing at the national level?

No there are no special requirements regarding data processing at the national level.

(iv) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

Yes. As stated above, in Article 23 of the GDPR the EU legislator has provided for the possibility to restrict the scope of the obligations and rights, including the information rights. Such limitations may have been introduced in specific legislation. The Polish legislator made use of this possibility by adopting the following restrictions.

The Act on the Protection of Personal Data provides in Articles 3 to 5a several restrictions with regard to exercise of data subject's right, as follows:

"Article 2

1. The provisions of Articles 5-9, Article 11, Articles 13-16, Articles 18-22, Article 27, Article 28 para. 2-10 and Article 30 of the Regulation 2016/679 shall not apply to activities consisting in editing, preparing, creating or publishing press materials within the meaning of the Act of 26 January 1984 - Press Law (Journal of Laws, item 24, as amended), as well as the statements made as part of literary or artistic activities.

2. The provisions of Article 13, Article 15 para. 3 and 4, Article 18, Article 27, Article 28 para. 2-10 and Article 30 of the Regulation 2016/679 shall not apply to academic expression.

Article 3.

1. The controller performing a public task shall not convey information referred to in Article 13 para. 3 of the Regulation 2016/679 if a change in the purpose of processing serves the performance of a public task and non-fulfilment of the obligation referred to in Article 13 para. 3 of the Regulation 2016/679 is necessary to fulfil the purposes referred to in Article 23 para. 1 of that Regulation, and conveyance of that information:

1) shall make it impossible or shall significantly hinder the performance of a public task, and the interest or fundamental rights or freedoms of the data subject are not superior with respect to the interest ensuing from the performance of that public task or

2) shall infringe the protection of classified information.

2. In the case referred to in para. 1, the controller shall implement appropriate measures to protect the interest or fundamental rights and freedoms of the data subject.

3. The controller shall be obliged to inform the data subject at its request, without undue delay, not later though than within one month of the day on which such request is received, about the grounds for not conveying the information referred to in Article 13 para. 3 of the Regulation 2016/679.

Article 4.

1. In matters not regulated in Article 14 para. 5 of the Regulation 2016/679, the controller performing a public task shall not convey information referred to in Article 14 para. 1, 2 and 4 of the Regulation 2016/679 if this serves the performance of a public task and non-fulfilment of the obligation referred to in Article 14 para. 1, 2 and 4 of the Regulation 2016/679 is necessary to fulfil the purposes referred to in Article 23 para. 1 of that Regulation, and conveyance of that information:

1) shall make it impossible or shall significantly hinder the performance of a public task, and the interest or fundamental rights or freedoms of the data subject are not superior with respect to the interest ensuing from the performance of that public task or

2) shall infringe the protection of classified information.

2. In the case referred to in para. 1, the controller shall implement appropriate measures to protect the interest or fundamental rights and freedoms of the data subject.

3. The controller shall be obliged to inform the data subject at its request, without undue delay, not later though than within one month of the day on which such request is received, about the grounds for not conveying the information referred to in Article 14 para. 1, 2 and 4 of the Regulation 2016/679.

Article 5.

1. The controller performing a public task shall not convey information referred to in Article 15 para. 1-3 of the Regulation 2016/679 if this serves the performance of a public task and non-fulfilment of the obligations referred to in Article 15 para. 1-3 of the Regulation 2016/679 is necessary to fulfil the purposes referred to in Article 23 para. 1 of that Regulation, and fulfilment of those obligations:

1) shall make it impossible or shall significantly hinder the performance of a public task, and the interest or fundamental rights or freedoms of the data subject are not superior with respect to the interest ensuing from the performance of that public task or

2) shall infringe the protection of classified information.

2. In the case where fulfilment of the obligations referred to in Article 15 para. 1 and 3 of the Regulation 2016/679 would involve a disproportionate effort associated with retrieving the personal data, the controller performing a public task shall ask the data subject for information making it possible to retrieve those data. The provision of Article 64 of the Act of 14 June 1960 - Code of Administrative Procedure (Journal of Laws of 2017, item 1257, and of 2018, items 149 and 650) shall apply accordingly.

3. In the cases referred to in para. 1 and 2, the controller shall implement appropriate measures to protect the interest or fundamental rights and freedoms of the data subject.

4. The controller shall be obliged to inform the data subject at its request, without undue delay, not later though than within one month of the day on which such request is received, about the grounds for not fulfilling the obligations referred to in Article 15 para. 1-3 of the Regulation 2016/679.

Article 5a.

1. The controller who received personal data from an entity performing a public task does not comply with the obligations referred to in Article 15 para. 1 and 3 of the Regulation 2016/679 in case where the entity transferring personal data made a request in this regard due to the need for proper performance of a public task aimed at:

1) the prevention, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

2) the protection of the State's economic or financial interests which includes in particular:

a) realizing and claiming revenues from taxes, payments, tax-exempt budget receivables and other receivables,

b) carrying out administrative enforcement of pecuniary and non-pecuniary receivables as well as securing pecuniary and non-pecuniary receivables,

c) preventing the use of the activities of banks and financial institutions for the purposes related to tax frauds,

d) disclosure and recovery of assets threatened with forfeiture in connection with offences,

e) performing inspections, including customs and fiscal inspections.

2. In the case referred to in para. 1 the controller shall reply to the request lodged on the ground of Article 15 of the Regulation 2016/679 in a way which allows to establish that the controller is processing personal data received from the entity performing a public task."

Notwithstanding with the above restrictions, it is perhaps worth mentioning that in the Polish legal framework there are some sectoral provisions regulating the specific procedure for the exercise of the right of access to certain information, e.g. to medical records, which constitutes a separate right of the patient, in addition to the right of access to data under the GDPR.

The realisation of access to medical records takes place on the principles and in the manner specified by the Act on Patient's Rights and Patient Ombudsman in the manner specified in its article 27 and the Regulation of the Minister of Health of 9 November 2015 on the types of scope and models of medical records and the manner of their processing. When providing the patient with access to medical records, the provider must not interfere with their content. When providing access to medical records, the way in which they are made available in the form set out in Article 27(1) of the Act on Patient's Rights, i.e. by, for example, making a copy, extract or printout.

In turn, providing access to a copy of the data contained in medical records, pursuant to Article 15(3) of the GDPR, is not synonymous with the obligation to provide access to data in a form and structure appropriate for providing access to medical records. The controller is also not obliged to provide the person concerned with access to the medium on which the personal data are processed and to data which do not constitute personal data within the meaning of Article 4(1) of the GDPR and do not concern the person seeking entry. When implementing the obligation under Article 15(3) of the GDPR, the data controller may only indicate the content of the data relating to the person concerned, to the exclusion of other information contained in the medium.

The performance of the obligation pursuant to Article 15(3) of the GDPR may therefore be accomplished both by making a copy or an extract of a document (medium) containing personal data and other data and by providing the authorised person with the contents of his/her personal data, excluding information contained in the medium which are not personal data within the meaning of Article 4(1) of the GDPR.

(See the article explaining the differences published on the Polish SA's website in Polish: https://uodo.gov.pl/pl/138/440).

21.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

No, there are no additional rules beyond the ones enforced by the GDPR for processing special categories of personal data in the Polish Act on the Protection of Personal Data.

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

No, there are not additional special rules when processing personal data of children, provided by the Polish Act on the Protection of Personal Data, beyond those specified in the GDPR.

The Polish legislator has not changed the age threshold set by the GDPR. Thus, in Poland, in relation to offering information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

However, the provision of art. 8 of the GDPR does not establish a general rule regarding children's consent to the processing of their personal data, as it only refers to child's consent expressed in relation to information society services.

Article 8(3) of the GDPR provides that paragraph 1 of this provision shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child. In Poland such provisions are the provisions of the Civil Code relating to capacity.

Therefore, when it comes to general child's consent for processing his or her personal data, the Act of 23 of April 1964 of the Civil Code shall be in use.

According to Article 11 of the Civil Code, full capacity for legal acts is acquired at the moment of becoming an adult – which means any individual who has attained eighteen years of age. In accordance with Article 12 individuals who have not attained thirteen years of age and persons fully legally incapacitated do not have capacity for legal acts.

Based on Article 14, a legal act performed by a person who does not have capacity for legal acts is invalid. However, if a person who does not have capacity for legal acts executes a contract of a type commonly executed in minor current day-to-day matters, this contract becomes valid the moment it is performed unless it causes serious harm to the person who does not have capacity for legal acts.

According to Article 15 minors who have attained thirteen years of age and persons partially legally incapacitated have limited capacity for legal acts.

In accordance with Article 17, subject to the exceptions provided for by the law, to be valid, a legal act whereby a person with limited capacity for legal acts assumes an obligation or disposes of his right requires the consent of his statutory representative).

(iii) Are there other vulnerable individuals identified in your national legislation?

No, there are no other vulnerable individuals identified in Polish legislation.

21.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

In Poland, there are no additional data protection rules applying to processing of personal data of deceased individuals. As recital 27 clarifies, the GDPR does not apply to deceased individuals.

However, the fact that deceased data is not considered personal data does not mean that information about deceased persons is deprived of legal protection in Poland. The protection of such data can be carried out e.g. under civil law, but the entity that may receive such protection is not the deceased, but their relatives, under the protection of personal rights as protection of the cult of memory of the deceased.

In addition, specific rules may provide for the protection of certain types of information regardless of whether that information concerns living or deceased persons. This is the case, for example, of the protection of information covered by medical secrecy (or even more broadly: secrets of the medical profession) - information concerning a patient is protected also after that person's death.

21.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

No the Polish regulation does not introduce any further provisions related to general accountability.

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

In accordance with Article 35(4) of the GDPR the Polish Supervisory Authority established and made public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.

As a rule, the processing which meets at least two of the below mentioned criteria will require a DPIA. In some cases the data controller can, however, consider that the processing which meets only one of the below mentioned criteria will require a DPIA. The more criteria are met by the processing, the more likely it is to result in a high risk to the rights and freedoms of data subjects, and in consequence, regardless of the security measures envisaged for application by the controller, a DPIA will be required.

The list of the kind of processing operations which are subject to the requirement for a data protection impact assessment refers also to data processing in research in different areas, giving examples of operations/ scope of data/circumstances, in which specific type of operation is likely to result in a high risk.

The English version of the list containing the types of processing operations which in the opinion of the Personal Data Protection Office require a DPIA is available here: https://edpb.europa.eu/sites/default/files/decisions/pl-dpia-list_monitor_polski.pdf).

Please also see the EDPB's Opinion on the draft list of the kind of processing operations which are subject to the requirement for a data protection impact assessment Opinion 17/2018 on the draft list of the competent supervisory authority of Poland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Please note that the list that has been updated to take account of the opinion issued by the European Data Protection Board and also covers processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or which may substantially affect the free movement of personal data within the European Union (issues relating to research remained unchanged). https://monitorpolski.gov.pl/MP/2019/666.

21.2 Commercialization of data

21.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
General Data Protection Regulation (GDPR).	https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en	Regulation (EU) 2016/679 of the European Parliament and of the Council	In Poland the main regulatory tool addressing data protection issues, including data commercialization, is the GDPR.
The Constitution of the Republic of Poland of 2nd April 1997	The Constitution of the Republic of Poland	Hard law	The Constitution of the Republic of Poland establishes guarantees concerning the right to privacy and protection of personal data (Articles 47 and 51).
The Act of 10 May 2018 on the Protection of Personal Data (In Polish: Ustawa o Ochronie Danych Osobowych)	The Act of 10 May 2018 on the Protection of Personal Data (English version)	Hard law	The Act of 10 May 2018 on the Protection of Personal Data is a Polish law, adopted by the Polish Parliament, regulating legal issues related to the protection of personal data, in

			particular ensuring the application of the provisions of the General Data Protection Regulation (GDPR).

Main regulatory tools addressing data commercialization.

21.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

Yes, if such processing is lawful under the GDPR

(ii) Do you know if these practices are routinely performed?

Yes, such practices are commonly used by the companies and usually involve the exchange of personal data for services (e.g. gaining access to an app) or benefits (e.g. discounts for signing up to a newsletter).

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

No, there is no such regulation.

(iv) Do you have any particular national regulation on the secondary use of data?

There is no particular national regulation on the secondary use of data.

However, there in the Act of 25 February 2016 on the re-use of public sector information that implements Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

(v) Do you have any specific protection for metadata or non-personal data in your country?

There is no national legislation with regard to non-personal data in Poland. The provisions of Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union applies directly.

21.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

The Polish Act of Personal Data Protection does not introduce any additional construct for data.

Based on the definition specified in the GDPR, data is an information.

For the information to be considered personal data it is generally irrelevant how the information is presented (expressed, communicated) or the medium on which the information is recorded (fixed). Personal data can be information presented by means of words, numbers (numbers), sounds, images, or it can be a combination of the above-mentioned forms (e.g. video recording). Personal data may be recorded both on traditional (paper) and IT carriers (e.g. computer disks, memory cards, pendrive type devices), however more and more often these are carriers over which the entity collecting this kind

of information does not have the actual authority (e.g. data recorded on the server in the network, "in the cloud"). The qualification of information as personal data shall not be affected by the fact that the information is false or contains errors; however, the provisions on the personal data protection impose the obligation to ensure that the information is correct and updated when necessary (cf. Article 5).

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

Yes, these are:

1. Act of 4 February 1994 on Copyright Act and Neighbouring Rights (machine translation of the Act). Unless otherwise provided by law, the author shall have the exclusive right to use and dispose of the work in all fields of exploitation and to remuneration for the use of the work. The Act determines the principles of remuneration for the author and his/her heirs.;

2. Act of 30 June 2000 on Industrial Property Law. (Official English translation: https://uprp.gov.pl/sites/default/files/_gAllery/38/29/38294/Industrial_Property_Law_as_amended_by_act_of_23_January_2004_and_act_of_29_June_2007.doc). This Act defines, among others, the relations with respect to inventions, utility models, industrial designs, trademarks, geographical indications and topographies of integrated circuits; and the rules under which entrepreneurs may accept rationalisation projects and reward their creators. Under the conditions specified in the Act, the author of an invention, utility model, industrial design and topography of an integrated circuit is entitled to remuneration.

21.3 Security and cybersecurity

21.3.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Act of 5 July 2018 on the national cyber security system	https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf (in Polish)	Hard law	Act of 5 July 2018 on the National Cybersecurity System implementing the provisions of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive").Yes, the technical and organisational

			measures has been implemented (see the answer to question 2 below).
Republic of Poland Cyber Security Strategy 2019-2024	https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8 (in English)		
Soft Law	The document sets out the strategic objectives and the relevant policy and regulatory measures that need to be implemented to make information systems, key service operators, critical infrastructure operators, digital service providers and public administrations resilient to cyber threats.		

Main regulatory tools addressing security and cybersecurity in Poland

21.3.2 Implementation of EU Law

(i) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

As stated above, the NIS Directive has been implemented in Poland by the Act of 5 July 2018 on the National Cybersecurity System.

(ii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

Yes, please find below examples of such provisions.

The public entities indicated in the Act and sectoral cyber security teams process data acquired in relation to cyber security incidents and threats, including personal data, covering also special categories of data referred to in Article 9(1) of the GDPR, to the extent and for the purpose necessary to perform the tasks set out in Article 26(3)(1)-(11), (14) and (15) and (5)-(8) and Article 44(1)-(3) of the Act.

The legislator pointed out in Article 39(2) of the Act on the National Cybersecurity System that in relation to the processing of special categories of data the entities mentioned therein shall carry out a risk analysis, apply measures to protect against malicious software and access control mechanisms, as well as develop procedures for secure exchange of information.

However, it should be pointed out that this is only of informative character as these obligations, in the light of personal data protection law, concern data processing regardless of its nature.

Moreover, Article 39(5) introduces the obligation to delete or anonymise the collected data by the designated entities and the sectoral cyber security team immediately after it has been established that they are not necessary for the performance of tasks referred to in Article 26(3)(1)-(11), (14) and (15) and (5)-(8) and Article 44(1)-(3).

Furthermore, the legislator has introduced a data retention period after the incident handling has been completed, which has been set at 5 years.

21.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

The general rules regarding personal data breach notifications are specified in Article 33 of the GDPR.

The Act on the Protection of Personal Data additionally sets out in Article 55 that the President of the Office may operate an ICT system allowing the controllers to notify any case of a personal data breach referred to in Article 33 of the Regulation 2016/679.

The procedure of notification of a personal data breach to the supervisory authority has been specified on the website of the Personal Data Protection Office: https://uodo.gov.pl/en/573/935 (English version).

The personal data breach notification is not explicitly regulated in the Act on the National Cybersecurity, implementing the NIS Directive. Both Directive and the Act establishes security and incidents (not personal data breaches) notification requirements for operators of essential services and for digital service providers.

According to Article 2 of the Act "incident" means "an event that has or may have an adverse impact on cyber security" whilst incident "handling" means "activities to detect, record, analyse, classify, prioritise, take corrective action and reduce the impact of an incident".

21.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or

something similar established? If yes, what are the competences and responsibilities?

(ii) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

The Act on the National Cybersecurity has introduced a decentralised model for determining the competent authorities for cyber security. The NIS Directive leaves this issue to the Member States. This is because Article 8 of the NIS Directive states that each Member State shall designate one or more national competent authorities for the security of networks and information systems, covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may designate an existing body or bodies to carry out this role.

The Polish legislator, taking into account the horizontal and hierarchical structure of the Polish public administration, has decided to base the system of competent authorities on ministers (excluding the Polish Financial Supervision Authority), as the chief administrative body. This is supported by the fact that these bodies have adequate legal capacity and resources necessary to effectively carry out the tasks entrusted to them. Such a requirement is introduced by Article 8(5) of the NIS Directive, which states that Member States shall ensure that competent authorities and points of single contact have adequate resources so that they can perform their tasks efficiently and effectively in order to achieve the objectives of this Directive. Member States shall ensure that the designated representatives cooperate efficiently, effectively and securely in the cooperation group.

The national legislator has therefore opted for a fragmented model of competent authorities, in which this function is performed by several authorities, dealing with matters substantively corresponding to the specificities of the operation of key service operators and digital service providers.

Thus, in accordance with Article 41 of the Act, the competent authorities for cyber security are:

1. for the energy sector - the minister in charge of energy;

2. for the transport sector excluding the water transport subsector - the minister in charge of transport;

3. for the water transport subsector - the minister in charge of maritime economy and the minister in charge of inland waterway transport

4. for the banking sector and financial markets infrastructure - the Financial Supervision Commission

5. for the health care sector excluding the entities referred to in Article 26(5) - the minister in charge of health matters

6. for the health sector including the entities referred to in Article 26(5) - the Minister of National Defence

7. for the drinking water supply and distribution sector - the minister relevant for water management;

8. for the sector of digital infrastructure excluding the entities referred to in Art. 26 par. 5 - the minister in charge of information technology

9. for the sector of digital infrastructure including the entities referred to in Art. 26 par. 5 - the Minister of National Defence;

10. for digital service providers excluding the entities referred to in Article 26 (5) - the minister in charge of informatization;

11. for digital service providers including the entities referred to in Article 26 (5) - the Minister of National Defence.

12. Pursuant to paragraph 7 of the commented provision, competent authorities for cyber security and the Single Point of Contact shall cooperate with law enforcement authorities and the competent authority for the protection of personal data, as appropriate.

This provision implements Article 8(6) of the NIS Directive, according to which competent authorities and the Single Point of Contact shall, where appropriate and in accordance with national law, consult and cooperate with relevant national law enforcement authorities and national data protection authorities.

The importance of cooperation is highlighted in recital 62 of the NIS Directive, which indicates that incidents may result from criminal offences in respect of which the prevention, investigation and prosecution is supported by coordination and cooperation between key service operators, digital service providers, competent authorities and law enforcement authorities. Where an incident is suspected to be connected to serious criminal offences under Union or national law, Member States should encourage key service operators and digital service providers to report serious criminal incidents to the relevant law enforcement authorities. Where appropriate, coordination between competent authorities and law enforcement authorities from different Member States should be facilitated by the European Cybercrime Centre (EC3) and ENISA.

The competent authority for the protection of personal data is the President of the Data Protection Authority. Law enforcement authorities include the Public Prosecutor's Office, the Police, the Border Guard, the Military Police, the Central Anticorruption Bureau, the Internal Security Agency and the National Tax Administration.

The Act on the National Cybersecurity, and executive regulations, issued based on it, set out in detail the obligations of individual entities in respect of detecting, recording, analysing and classifying incidents, as well as the requirements concerning the manner of reporting incidents, the manner of coordinating the handling of incidents (meaning activities that enable detecting, recording, analysing, classifying, prioritising, taking corrective action and reducing the effects of an incident), of the respective entities, as well as the amount of and manner of imposing fines in the event of a violation of the provisions of the Act..

21.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment? Are there administrative fines related to data protection issues?

With reference to the Act on the protection of personal data – it provides both administrative and criminal liability (as well as the civil liability for the infringement of personal data protection provisions and proceedings before court);

In accordance with article 101 of the Act on the protection of personal data the President of the Office may impose on the entity obliged to comply with the provisions of the Regulation 2016/679, other than: entity of the public finance sector, research institute or the National Bank of Poland - by way of a decision, an administrative fine on the basis of and on terms and conditions stipulated in Article 83 of the Regulation 2016/679.

In accordance with Article 102 of the Act the President of the Office may, by way of a decision, impose administrative fines in the amount of up to PLN 100,000.00 on: entities of the public finance sector referred to in Article 9 (1-12) and 14 of the Act of 27 August 2009 on Public Finance, research institute and the National Bank of Poland. The President of the Office may also, by way of a decision, impose administrative fines in the amount of up to PLN 10,000.00 on entities of the public finance sector referred to in Article 9 (13) of the Act of 27 August 2009 on Public Finance.

The administrative fines shall be imposed by the President of the Office on the basis of and on terms and conditions stipulated in Article 83 of the Regulation 2016/679.

Additionally, in accordance with Article 107 of the Act on the protection of personal data any person who processes personal data, although processing thereof is not permitted, or is not authorized to process them, shall be subject to a fine, restriction of personal liberty or imprisonment for up two years.

If the act referred to in para. 1 pertains to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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, shall be subject to restriction of personal liberty or imprisonment for up three years.

Article 108 states that any person who prevents or hinders the inspector from checking the compliance with the personal data protection provisions shall be subject to a fine, restriction of personal liberty or imprisonment for up to two years.

The same sanctions shall apply to any person who in connection with the pending proceedings in the case of imposing an administrative fine does not provide the data necessary to determine the basis of assessment of administrative fine or who provides the data which make it impossible to determine the basis of assessment of administrative fine.

What is more, in accordance with Article 92, in matters not regulated in the Regulation 2016/679, the provisions of the Act of 23 April 1964 - Civil Code - shall apply to claims related to the infringement of the personal data protection provisions referred to in Article 79 and Article 82 of that Regulation.

With reference to the cybersecurity, the Act on the National Cybersecurity System indicates specific provisions on fines in Chapter 14 of the Act.

Fines are imposed in the form of an administrative decision by the authorities competent in the field of cybersecurity specified in Chapter 8 (the minister in charge of energy, the minister in charge of transport, the minister in charge of maritime economy, the minister in charge of inland navigation, the Banking Supervision Commission, the minister in charge of health, the Minister of National Defence, the minister in charge of water management and the minister in charge of informatisation).

Do data protection offences constitute an official offence or are only prosecuted by the injured party's request

(ii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

The President of the Personal Data Protection Office, as a national supervisory authority, is competent to conduct proceedings in cases of data breaches of personal data. The proceedings may be initiated on the basis of the findings made during the inspections, which indicate that the personal data protection regulations may have been breached, or by

obtaining such information from other sources (e.g. from media reports), or by a complaint of the data subject.

21.5 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

Please note that the conditions for conducting clinical trials on medicinal products are regulated in Poland by the Pharmaceutical Law of 6 September 2001. Each clinical trial can be conducted only on the basis of a previously issued permit by The President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products and a positive opinion of the bioethics committee. The President of the Office makes an entry of the clinical trial to the Central Register of Clinical Trials. According to the Pharmaceutical Law Act, a clinical trial of an investigational medicinal product is conducted in accordance with Good Clinical Practice, which provides a standard that defines the way in which the results of clinical trials conducted with the participation of humans are planned, conducted, monitored, documented and reported. [the text of the Act in Polish]

The Good Clinical Practice is regulated by the Regulation of the Minister of Health of 2 May 2012 on Good Clinical Practice. The document regulates the obligations of the investigator and the sponsor in the context of a clinical trial. It sets out the rules for creating the clinical trial protocol, the investigator's brochure and the clinical trial agreement [text of the Regulation in Polish].

According to the provisions of the Pharmaceutical Law Act, the President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products exercises control over the conduct of clinical trials. To streamline the work of the President, the Medicinal Products Inspection Department was established in 2011. Inspections can be conducted on a national basis and by order of the European Medicines Agency. The inspection may concern the site, the premises of the sponsor, the clinical trial organisation conducting the clinical trial on request (CRO) or other recognised sites. The procedure and detailed scope of conducting clinical trial inspections are specified in the Regulation of the Minister of Health of 26 April 2012 on Clinical Trial Inspections (text of the Regulation in Polish).

The Central Register of Clinical Trials is a data register maintained in the form of an IT system by the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products. Information on each new registered clinical trial is entered into the Central Register of Clinical Trials that includes:

- title of the clinical trial;
- the clinical trial protocol number;

- the clinical trial number in the European clinical trials database (EudraCT);
- The names and addresses of the trial sites where the clinical trial is being performed;
- identification of the phase of the clinical trial;
- name of the investigational medicinal product;
- name of the active substance;
- number of clinical trial participants;
- characteristics of the groups of clinical trial participants;
- name, surname and place of residence or registered office of the sponsor;
- name, surname and title and degree of the investigator;
- name, surname and title and degree of the clinical trial coordinator, if involved;
- the date of notification of the clinical trial;
- date of the end of the clinical trial;
- clinical trial decision information;
- clinical trial number in the Central Register of Clinical Trials.

I am not aware of any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes. However, as states above, according to the provisions of the Pharmaceutical Law Act, the President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products exercises control over the conduct of clinical trials..

22 Portugal

Vera Lúcia Raposo (Macau University, University of Coimbra) Carla Barbosa (University of Coimbra)

Brief report on the implementation of the GDPR in Portugal

More than one year after the entry into force of the General Data Protection Regulation ("GDPR"), Law n. 58/2019 (hereafter, Law on Data Protection) was published on August 8, 2019, to ensure the implementation of the RGPD in the Portuguese legal order.

The delay in the transposition of the Regulation was due to delays in its drafting. Moreover, disagreements between the Government, the National Data Protection Commission (CNPD) and the members of the national Parliament created additional difficulties to the legislative process.

Law n. 58/2019 repealed the former law on personal data protection, Law n. 67/98 of 26 October, and amended the law on the organization and functioning of the National Data Protection Commission ("CNPD"), Law No. 43/2004 of 18 August.

Law n. 58/2019 contains some minor specifications of the GDPR. Among the various specificities of the Portuguese law, the most relevant relates with fines. According with the GDPR, in the most severe cases of non-compliance fines can reach up to 20 000 000 euros or 4% of the company's annual gross revenue in global terms from the preceding year,