The role of UREC-E is to audit research ethics self-assessment and ethical reviews carried out by FRECs.

The role of UREC-DP is to:

- liaise with the Malta Information and Data Protection Commissioner (IDPC) in terms of Section 7 of Chapter 586 of the Laws of Malta (Data Protection Act 2018) to obtain any necessary authorisation required for research proposals that have been referred to it;
- review research proposals, referred to it by the FRECs, that deal with special categories of personal data as defined in the GDPR.;
- carry out annual audits of research data protection self-assessments carried out by Researchers and reviews carried out by FRECs on data protection matters not related to special categories of personal data to ascertain that self-assessments and reviews are consistent with the policies approved by Senate, the GDPR, and Chapter 586 of the Laws of Malta (Data Protection Act 2018); (d)Prepare an annual report to Senate summarizing activities carried out, including the results of the audit.

There are no specific provisions in the Research Code on R&I activities related to dual use or security-sensitive technologies.

20 Netherlands

Ernst Halberstadt (Independent researcher)

20.1 Informed consent

20.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Grondwet (Constitution)	https://wetten.overheid.nl/BWBR0001840/2018-12-21	Constitution	art. 10 enshrines the constitutional right to privacy and data protection
Algemene Verordening Gegevensbescherming (AVG/GDPR)	https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679	Hard law	Directly applicable in the Netherlands. Supersedes Wet bescherming persoonsgegevens (Wbp) which was the national implementation of the Privacy and Data Protection Directive '95

Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)	https://wetten.overheid.nl/BWBR0040940/2018-05-25	Hard law	Where the GDPR (AVG) leaves room for discretionary power of the member state UAVG provides these national choices.
Burgerlijk Wetboek (BW)	https://maxius.nl/burgerlijk-wetboek-boek-1/artikel435/ https://wetten.overheid.nl/zoeken/zoekresultaat/rs/2/titel/burgerlijk%20wetboek/titelf/1/tekstf/1/artnrb/0/d/07-10-2019/dx/0	Hard law	General concept of consent in civil law
Telecommunicatiewet (Telecommunication Act)	https://wetten.overheid.nl/BWBR0009950/2019-01-01	Hard law	Regulates consent, spam prohibition, cookies for electronic communication. Has the following legislative regulation incorporated: Directive 2002/21/EC (Regulatory Framework for electronic communications networks and services Directive 2002/58/EC, as amended by Directive 2009/136/EC. (ePrivacy Directive)

Wet politiegegevens (Wpg)	https://wetten.overheid.nl/BWBR0022463/2019-07-01	Hard law	Regulates the processing of personal data by the National Police, Military Police, Intelligence Apparatus, Bureau of Investigation
Wet justitiële en strafvorderlijke gegevens (Wjsg)	https://wetten.overheid.nl/BWBR0014194/2019-05-01	Hard law	Regulates the processing of judicial data (in personal files) and for the official Certificate of Conduct
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/BWBR0023864/2019-07-01	Hard law	Regulates the use of national ID-numbers in the healthcare sector
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	https://autoriteitpersoonsgegevens.nl/nl	Soft law (however enforced	Rules around privacy and data protection. Website provides the 'translation' of the relevant privacy

Authority (AP)		by AP on sanction of fines)	and data protection legislation and their applicability into daily practice.

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

(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?

Art. 10 Grondwet enshrines the constitutional right to privacy and data protection, including application to the purely personal and household activities. The UAVG does not provide any such exception.

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

Wet beveiliging netwerk- en informatiesystemen (Wbni)[128] regulates data breaches or loss of integrity of electronic information systems and regulates the processing of data in the framework of the competencies of the Minister of Security and Justice. It should be noted that it is applicable only to providers of products and services that are of vital interest to the Dutch society[129]

Wet politiegegevens (Wpg)[130] regulates the competencies of the enforcement authorities with regard to the processing of personal data in case of the occurrence of national security threats.

In addition to the Criminal Code (Wetboek van Strafrecht)[131] and the Criminal Procedural Code (Wetboek van Strafvordering)[132], the Wet computercriminaliteit III[133] regulates the competencies of the executive and judiciary branch (trias) in the framework of (organized) cybercrime and national security threats.

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public

[128] Available at https://wetten.overheid.nl/BWBR0041515/2019-01-01
[129] Art. 3 jo. 5 Wet beveiliging netwerk- en informatiesystemen
[130] https://wetten.overheid.nl/BWBR0022463/2019-07-01
[131] https://wetten.overheid.nl/BWBR0001854/2019-08-01
[132] https://wetten.overheid.nl/BWBR0001903/2019-08-01
[133] https://zoek.officielebekendmakingen.nl/stb-2018-322.html

Autoriteit Persoonsgegevens (AP)	https://www.autoriteitpersoonsgegevens.nl/	yes	158 (January 2019)	Despite a recent doubling of the budget, very limited enforcing capacity due to understaffing	AP acts primarily on the basis of complaints filed by the public.
Autoriteit Consument & Markt (ACM)	https://www.acm.nl/	yes	520 (divided in market sectors)	Very active in general. Related to Telecommunications Act, ACM fines organisations on a regular basis for non-compliance with the Telecommunications Act.	Investigation initiates from complaints from the public or anonymous informants

Information regarding Data Protection Authorities, Netherlands

(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.?

In line with the GDPR, art. 24, 28 and 32 UAVG provide exemptions to the prohibition of processing of special categories of personal data for scientific or historic research purposes, or public interest purposes. However, 'data processing for research purposes', nor 'research in public interest' are further defined, neither in the Explanatory memorandum to the draft law[134], neither are there made any references to Ministerial lists of expected research.

(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?

[134] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming/Memorie+van+toelichting+wetsvoorstel+Algemene+verordening+gegevensbescherming.pdf

In line with the GDPR, art. 24 UAVG provides exemptions to the prohibition of processing of special categories of personal data for scientific or historic research purposes, or statistical purposes. For the processing to be eligible for the exemption it is needed that the processing is necessary for the intended research, **and**, serves the public interest, **and**, the acquirement of all the required consent is an impossibly large task, **and**, measures have been taken to prevent disproportionate harm to the rights and freedoms of the data subject (art. 24 UAVG).[135] The UAVG however does not further specify what measures need to be taken and does not mention data protection assessments or privacy by design measures etc.

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

Art. 30 par. 3 UAVG provides exemptions from the prohibition to process special categories of personal data for medical personnel, insurers, attorneys are professionals that work under a NDA.

The Wet politiegegevens[136] provides a number of additional rules to the processing of special categories of personal data with regard to authorisations (art. 6), automated search (art. 11), retention (art. 14), distribution to third parties (art. 18,19, 36e). The Wpg also makes a distinction between erasing and destroying personal data, there erasure means that personal data is erased from the visibility of the system, but not in its entire existence.

(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.)?

On instigation of the Ministry of Education and the State's Social-Scientific Advisory Council, the Association of Dutch Universities (Verenigde Universiteiten -VSNU) published a Code of Conduct (approved by the DDPA) for the processing of personal data in scientific research.

This Code of Conduct[137] (hereafter: 'The Code') aims at processes of personal data in the context of scientific research conducted by employers of a. Dutch universities, and b. other organizations that carry out scientific research and registered themselves at VSNU to publicize their compliance with the Code.

The Code requires the adhering parties to perform a range of organizational and technical measures and conform to a set of data processing principles.

The Code also contains a provision for an arbitration body from VSNU[138].

[135] https://wetten.overheid.nl/BWBR0040940/2019-02-19

[136] https://wetten.overheid.nl/BWBR0022463/2019-07-01

[137] https://www.vsnu.nl/files/documenten/Domeinen/Accountability/Codes/Gedragscode%20persoonsgegevens.pdf

[138] Please note that a new version of the Code Of Conduct (incorporating the GDPR) is currently subject of consultation rounds amongst the stakeholders. https://www.vsnu.nl/files/documenten/Domeinen/Governance/Consultatieversie%20-%20VSNU%20Gedragscode%20voor%20gebruik%20van%20persoonsgegevens%20in%20wetenschappelijk%20onderzoek.pdf

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

The UAVG regulates "statistical purposes" in line with the respective regime of the GDPR. Art. 24 provides an exemption to the prohibition to process special categories of personal data for statistical purposes under the criteria of necessity, common interest, explicit consent and counterbalancing proportionate measures.

(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.)

There are no other references to data processing for research purposes in the Dutch national legislation besides the abovementioned.

However, there are a number of associations that are involved with monitoring statistical and data analytics research, that make use of a Code of Conduct or an Integrity Code[139] in which the data protection requirements for the stakeholders involved are further specified. Examples of such associations are the Center for Information Based Decision Making & Marketing Research (MOA)[140], the Association for Policy research (VBO)[141], the Association for Statistical research (VSO)[142], Vereniging van Universiteiten (VSNU).[143]

20.1.2 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.)

Jurisprudence constitutes the right for small enterprises (legal entities: 'eenmanszaak', 'zzp', 'stichting', 'vereniging') to enjoy certain provisions that are originally written for consumers. This legal construct is known as 'reflexwerking'. As such, these small enterprises may enjoy the legal provisions that data subjects of processing of personal data enjoy.

However, a reservation has to be made. The GDPR is aiming at protecting natural persons (and not consumers), whereas for example the Telecommunications Act provides a number of privacy and data protection provisions that are aimed at protecting consumers. The reflexwerking as such, only effects consumer protection provisions.

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

No. art. 7 GDPR is followed.

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

No. art. 5 and 6 GDPR are followed.

[139] See an example of an Integrity code that is used by MOA, VBO and VSO. http://vsonet.nl/wp-content/uploads/2018/08/MOAVSOVBO-Gedragscode-versie-14-defa.pdf
[140] https://www.moaweb.nl/
[141] https://www.beleidsonderzoek.nl/
[142] https://www.vsonet.nl/
[143] https://www.vsnu.nl/

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

subject's right that are provided by the GDPR.

Art. 45 UAVG cancels the right of access in case the request is aimed at archives that are enumerated under art. 1 sub c Archive Act[144], and, such request is not sufficiently detailed resulting in the unreasonability of carrying out the request.

Art. 47 UAVG cancels the effect of art. 15 (access), 16 (rectification), 18 (restriction) and 19 (notification obligation) of the GDPR in the context of public registries.

20.1.3 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)?

Besides the standard regime for exemptions from the prohibition to process special categories of personal data ex. Art. 22 par. 2 GDPR there is a number of additional rules.

Art. 30 par. 3 UAVG provides exemptions from the prohibition to process special categories of personal data for medical personnel, insurers, attorneys are professionals that work under a Non-Disclosure Agreement.

The Wet politiegegevens provides a number of additional rules to the processing of special categories of personal data with regard to authorisations (art. 6), automated search (art. 11), retention (art. 14), distribution to third parties (art. 18,19, 36e). The Wpg also makes a distinction between erasing and destroying personal data, there erasure means that personal data is erased from the visibility of the system, but not in its entire existence.

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

According to art. 5 para 1 UAVG the legal consent age for the processing of personal data in the Netherlands is 16. [145]

A recent amendment to the UAVG provides that minors do not need to be asked for consent in the case they ask for help from non-commercial advisory services (art. 5 para 5 UAVG)[146].

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

Under the UAVG individuals under guardianship enjoy the same provisions as minors (art. 5 UAVG).

20.1.4 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

[144] https://wetten.overheid.nl/BWBR0007376/2018-07-28. Art. 1 Archiefwet maintains a broad definition of archive material.

[145] https://autoriteitpersoonsgegevens.nl/nl/nieuws/mag-ik-onder-de-avg-gegevens-van-kinderen-verwerken#subtopic-5805

[146] https://wetten.overheid.nl/BWBR0040940/2019-02-19

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?

The UAVG is not applicable to deceased individuals, nor are there any provisions for the right of deletion of personal data of deceased individuals.

It is noteworthy that the regime in the medical sector is that relatives and heirs have no right to access to or deletion of the medical file of a deceased individual, unless consent may be assumed for example for a relative that was closely following the treatment procedure at first hand.[147]

20.1.5 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 accountability principle for privacy and data protection matters is only enshrined in the UAVG.

(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?

Besides the standard regime of the UAVG (in line with art. 35 of the GDPR) there is no other legislation that specifies when a data protection impact assessment is required and how it should be conducted.

For example, art. 4c and 33b Wet politiegegevens provide DPIA requirements that are in line with the standard regime of art. 35 the GDPR;

In case of probable high risk processing of personal data, a data protection impact assessment should be carried out and the assessment should contain at least the elements that are enumerated in art. 35 GDPR (description of the envisioned processing, assessment of the risks, measures to remediate the risks, preventive- and security measures and mechanisms to protect police data and adherence to the accountability principle.

20.2 Commercialization of data

20.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Telecommunicatiewet		Hard law	Consumer – and privacy protection legislation. Regulates

[147] Koninklijke Nederlandsche Maatschappij tot bevoredering der Geneeksunst (KNMG) is the federation of medical professional associations.
See KNMG general guidelines "processing medical data" under para 5.3.
https://www.knmg.nl/advies-richtlijnen/dossiers/medisch-dossier-overledene-beroepsgeheim.htm

			consent, spam prohibition and cookies for electronic communication
Dutch Civil code (book 7)		Hard law	Legislation on consumer sales
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 commercialization.

20.2.2 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)?

There is no specific regulation for the contractual exchange of personal data as a compensation for access to services. However, legislation about the boundaries of the terms and conditions of a contractual agreement (formal and material requirements) are specified in the Dutch Civil Code Book 6[148]. Art. 6:236 and 6:237 specify situations in which terms and conditions are suspected to be unreasonably onerous. A number of conditions may apply to the situation where personal data in exchange for access to services is contractually demanded, for example:

[148] https://wetten.overheid.nl/BWBR0005289/2019-07-21

6: 236 sub a: where the contractual party does not grant access to the service that was contractually agreed upon to the other party until the other party hands over a set of personal data.

6:236 sub r: where the contractual party does not allow the other party to withdraw from an agreement (or withdraw consent for access to certain personal data).

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

The boundaries of terms and condition of a contractual agreement are often tested by commercial parties and often trumped (as proven by an extensive list of court cases and judicial bodies related to the abovementioned articles). However, when it comes to the particular situation of contractual exchange of personal data in return for access to a service (in particular apps) one cannot speak of a practice routinely performed. It is indicative of the situation that on the website of the Data Protection Authority only two investigations over personal data in the context of app services are published (respectively from 2014 and 2015).

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

No specific regulation on the renumeration of data subjects.

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

Yes, there are exemptions made from the principle of purpose limitation for statistical and research purposes.

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

No, my expectation is that these aspects will be covered with the upcoming ePrivacy Regulation.

20.2.3 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?

There is no legislation or body that specifically classifies data. Data can be subject to the Auteurswet (Copyright Act) or Databankenwet (Database Act). Under the Auteurswet works of collected data may be protected when extensive enough and systematically and methodically organized (art. 10 para 3 Auteurswet[149]). Under the Databankenwet the manufacturer of a database enjoys protection when the data form a collection independent elements that are systematically or methodically organized and from which the presentation or handling of the collection proves a substantial amount of investment in qualitative and/or quantitative sense.[150]

(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?

To my knowledge the only mechanisms to determine the value of data are that of the Database Act and Copyright Act.

[149] https://wetten.overheid.nl/BWBR0001886/2015-07-01
[150] https://wetten.overheid.nl/BWBR0010591/2018-10-11

In Dutch law the basis for the determination of the remuneration of the manufacturer of the (artistic) work is based on the determination of damages (art. 27 Auteurswet[151] jo. 6:162 BW[152]). A Dutch court has the power to theoretically (in an abstract sense) estimate the damage (art. 27 para 2 Auteurswet jo. 6:97 BW). Viable determinations of damage are based on a) violation of the right to be mentioned as the manufacturer of a work (art. 25 Auteurswet) , b) loss of exclusivity and loss of exploitation possibilities, c) decrease of traffic to the website of the manufacturer, d) the impossibility to shape a user's-license, e) loss of income out of advertisement, f) time to map the violations.[153]

20.3 Security and cybersecurity

20.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Telecommunicatiewet	https://wetten.overheid.nl/BWBR0009950/2019-01-01	Hard law	Regulates the protection of citizens within every form of digital communication. Providers have to take appropriate technical and organizational measures to safeguard the use of their networks and services.
Wet computercriminaliteit (Wcc)	https://zoek.officielebekendmakingen.nl/stb-2018-322.html	Hard law	https://nl.wikipedia.org/wiki/Computercriminaliteit Regulates cybercrime in the form of additions to the Dutch Criminal Code and Criminal Procedure Code. Provides the regime to act against i.a. hacking, DoS-attacks, grooming. Also provides the powers (i.e. wiretapping) for the enforcement agencies to act against cybercrimes.
Wet beveiliging netwerk- en informatiesystemen (Wbni)	https://wetten.overheid.nl/BWBR0041515/2019-01-01	Hard law	Implementation of the EU Directive 2016/1148.154 Regulates data breaches or loss of integrity of electronic information systems and

[151] https://wetten.overheid.nl/BWBR0001886/2015-07-01
[152] https://wetten.overheid.nl/BWBR0005289/2019-07-21
[153] https://www.iusmentis.com/auteursrecht/inbreuk/schade-online-claim/#bepalingvanschade
[154] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

			regulates the processing of data in the framework of the competencies of the Minister of Security and Justice. It should be noted that it is applicable only to providers of products and services that are of vital interest to the Dutch society[155]
Wet Gegevensverwerking en Meldplicht Cybersecurity (WGMC)	https://wetten.overheid.nl/BWBR0039866/2018-05-01	Hard law	Regulates the powers and responsibilities of the National Cybersecurity Centre (NCSC) and defines how the NCSC should act in case of a digital security incident with a vital infrastructure provider.
Baseline Informatiebeveiliging Overheid	https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html	Binding guidelines	Binding guidelines for information security for public bodies. Based on ISO 27001/27002 standards.

Main regulatory tools addressing security and cybersecurity in Netherlands

20.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

Before the entry into force of the GDPR, the Data Breach Notification Act[156] contained a formal procedure to follow in case of an data breach incident. However, with the entree into force of the GDPR the Data Breach Notification Act was annulled, and the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) has since sufficed with a publication of guidelines for the public for notifying data breaches to the DDPA[157].

No further procedures are described in national regulation.

The National Cyber Security Centre (NCSC) is an independent leg of the Ministry of Justice and Security aimed at enhancing the resilience of Dutch society in the digital domain.[158] The NCSC publishes binding procedures and guidelines on their website.

The function of the NCSC will be further explained below under 3.3.

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

[155] Art. 3 jo. 5 Wet beveiliging netwerk- en informatiesystemen
[156] https://wetten.overheid.nl/BWBR0037346/2015-12-16
[157] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_kom_in_actie_bij_een_datalek.pdf
[158] https://www.ncsc.nl/

The NIS Directive is implemented by the Wet beveiliging netwerk- en informatiesystemen (Wbni), which entered into force in November 2018. It regulates data breaches or loss of integrity of electronic information systems and regulates the processing of data in the framework of the competencies of the Minister of Security and Justice. It should be noted that it is applicable only to providers of products and services that are of vital interest to the Dutch society[159]

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

Wet politiegegevens (art. 4a), Wet justitiële en strafvorderlijke gegevens (art. 7), Telecommunicatiewet (art. 11.3) all have a similar stipulation integrated, however derived not from the GDPR, but from respectively Directive (EU) 2016/680 and Directive (EU) 2002/58. In addition, several sectoral codes of conduct (i.e. in the 'Code of conduct for suppliers of smart energymeters' (Gedragscode Leveranciers Slimme Meter) in the energysector) also require appropriate technical and organizational measures.

20.3.3 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 NIS Directive is implemented by the Wet beveiliging netwerk- en informatiesystemen (Wbni).[160] In this regulation a provider of vital infrastructure (assigned as such by the Minister of Security and Justice) has the obligation to notify the Minister in case of a) an incident which compromises the continuity of the provider's vital service, or b) a security breach in the network- and information systems that compromise the continuity of the provider's vital service (art. 10 Wbni).

The criteria to determine the incident has consequences for the continuity of the vital service are a) the number of users that are hit by the disruption, b) the duration of the incident, c) the scale of the geographical area that is hit by the incident (art. 10 par.4 Wbni).

The notification should at least include a) the nature and scale of the incident, b) the suspected time of commencement, c) the potential consequences in- and outside the Netherlands, d) an estimation of the recovery time, e) the measures that the provider performed in order to limit the consequences and/or to prevent the incident from occurring again, f) contact data of the person responsible for notifying.

20.3.4 Supervision of cybersecurity

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

There is not one national supervisory body with enforcement powers. The National Cyber Security Centre (NCSC) functions as a Cyber Security Incident Response Team (CSIRT), warns for risks and offers assistance with cyberincidents.

[159] Art. 3 jo. 5 Wet beveiliging netwerk- en informatiesystemen
[160] https://wetten.overheid.nl/BWBR0041515/2019-01-01

Some sectors have appointed a sectoral supervisory body for the adherence of safety measures and the notification obligation, and have the power to enforce with sanctions and administrative fines. I.e. the supervisor in the banking sector is De Nederlandsche Bank[161], the supervisor in the telecom sector is Agentschap Telecom.[162]

(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?

The National Cyber Security Centre (NCSC) is an independent leg of the Ministry of Justice and Security aimed at enhancing the resilience of Dutch society in the digital domain.[163] More specifically, it aims at creating a safe, open and stable information society. The NCSC collects cyber security information from government, companies, universities and international contacts, and brings out advice for companies and public services to deal with ICT vulnerabilities. The NCSC disseminates via whitepapers, trend reports, fact sheets, and files about actual topics related to digital security.

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

There is no specific regulation for compensation remedy for damages resulting from cyber incidents. It is dealt with via the standard regime of tort.

20.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

Cybercrime is regulated in the Wet computercriminaliteit[164]. It regulates cybercrime in the form of additions to the Dutch Criminal Code and Criminal Procedure Code. As such, it provides a regime to act against i.a. hacking, DoS-attacks, grooming and other forms of cybercrime. It also provides the powers (i.e. wiretapping) for the enforcement agencies to act against cybercrimes and it provides legal basis for fines and imprisonment.

Imprisonment, community service and fines can be imposed. Fines can be imposed ranging from EUR 335,- to EUR 670.000[165]. Imprisonment can be imposed ranging from 1 week to 4 years[166]. Community service can be imposed ranging from 20 to 180 hours[167]. The basic assumption for every violation is that the incriminated individual restitutes the inflicted material damage[168].

(ii) Are there administrative fines related to data protection issues?

[161] https://www.toezicht.dnb.nl/en/3/51-203304.jsp
[162] https://www.agentschaptelecom.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen
[163] https://www.ncsc.nl/
[164] https://zoek.officielebekendmakingen.nl/stb-2018-322.html
[165] Art. 23 Wetboek van Strafrecht. https://wetten.overheid.nl/BWBR0001854/2019-08-01
[166] See sanctions guideline cybercrime of the public prosecutor https://www.om.nl/@101753/richtlijn-8/
[167] Id.
[168] Id.

Besides the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) which has its legal basis for administrative fines from the GDPR, competent supervisory authorities per sector are appointed (for an overview see art. 4 Wbni[169]) and are provided with the power to issue administrative fines via art. 29 Wbni.[170]

Recently the Dutch Data Protection Authority imposed its first administrative fine of EUR 460.000 on a hospital that was found non-compliant with art. 32 GDPR.[171]

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

It depends on the nature of the data protection offence if the violation is prosecuted ex officio or as a complaint offense.

Stalking, defamation and slander are examples of violations that are prosecuted by the injured party's request. If these types of violations are accompanied or carried out by acts of cyberhacking, then the acts of cyberhacking may be treated as a complaint offense.

However, in general, data protection offences constitute an official offense.

20.5 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?

Before the commencement of a (bio)medical science research project, the research project file has to be examined by one of the 19 Research Ethics Committees (REC's)[172] or by the Central Commission for person-related research (CCMO). The REC's or CCMO examine the research project and assess compliance with relevant regulations, several which contain data protection provisions.[173]

The main pieces of regulation are the GDPR and the Health-scientific research with persons Act ('Wet medisch-wetenschappelijk onderzoek met mensen' (WMO)) regulates health related scientific research with people as subjects. However, the only provision related to data protection is art. 29, which provides that special categories of personal data must be excluded from the research.

Furthermore, there is the Code of Conduct Health research[174] created by the Federation of Medical Scientific Associations (FMWV) - a cooperative platform for 8.000 researchers

[169] https://zoek.officielebekendmakingen.nl/stb-2018-387.html
[170] https://zoek.officielebekendmakingen.nl/stb-2018-387.html
[171] https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers
[172] https://www.ccmo.nl/metcs/erkende-metcs
[173] https://www.ccmo.nl/onderzoekers/wet-en-regelgeving-voor-medisch-wetenschappelijk-onderzoek/wetten
[174] https://www.federa.org/code-goed-gedrag

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