'Big data analytics' and processing of health data for scientific research purposes : the Dutch legal framework

Research Protocol by at MedLawconsult, Evert-Ben van Veen
in The Hague, The Netherlands

Contents

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

1. Overview of the legal framework

First, we would like to get an overview of the current and upcoming legal framework applying to the processing of health data for research purposes in your country.

a. Which laws regulate the processing of health data for research purposes (the current regime, in force till 25 May 2018)

What are the relevant applicable provisions governing the processing of health data in your country? Please provide online references (also to an English version, if available), a brief description and any specific relevant information.

The two most important laws are:

1. The Data Protection Act (Wet bescherming persoonsgegevens, WBP)[1];
2. The Act on Treatment Contract.

Ad 1:

This is the generic data protection Act, implementing Directive 95/46/EC. It follows the Directive quite diligently. It came into force in 2001 and succeeded the previous Act on the protection of registries containing personal data. The Act has been amended several times, yet leaving the basic structure intact. The last change was in 2015 when an obligation to notify data breaches to the Data Protection Authority, the Autoriteit Persoonsgegevens (AP), was introduced.[2]

Its impact on research will be discussed in paragraph 2.

Yet, one aspect should be mentioned here. Article 24 WBP states that a number which has been assigned by law to identify a data subject, can only be used for the purposes as stated by that law. The second section states that a Royal Decree can make exceptions.

There are several laws which designate the Dutch civic registration number ('burgerservicenummer', hereinafter: CRN) as the number to be used for identification and exchange with designated entities. In health care that is the Act on additional conditions for processing personal data in health care (Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, Wabvpz,[3] more about that Act infra at p.6). Insofar as relevant here, the Act states that the CRN must be used by and between health care practitioners to administer health care, by health insurers

[1] Act of July 6, 2000

[2] Entering into force on 1-1-2016, Staatsblad 2015, no. 230.

[3] Act of April 10, 2008

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

and in the interchange between health care providers[4] and health insurers (such as when bills are sent to the insurer).

There is not an Act or a Royal decree which states that the CRN can be used for research. Hence the CRN cannot be used to link records for research. In that case one must use either directly or indirectly identifiable data which paradoxically reveal more about the identity of a subject than the 9 digits of the CRN. A solution has been found to securely one way hash the CRN into a random number. If done by a 'trusted third party' (TTP) that TTP could repeat that procedure at the various data sources and data could be combined under that number in the research database. There is considerable debate whether such initial hashing should still be considered using the CRN for research. The majority of lawyers have the opinion that this is not using the CRN for research in a way which is incompatible with art.24 of the WBP. The AP has not given a formal opinion on this issue but implicitly seems to allow this.[5]

Ad 2:

The healthcare practitioner-patient relation is regulated in the Dutch Civic Code through a specific chapter. This chapter is generally known as the Act on the medical treatment contract or in Dutch, de Wet inzake de geneeskundige behandelingsovereenkomst (WGBO). It came into force in 1995[6] and since then has only been amended on small issues, one of them being the extension of the default period for retaining the medical file from 10 to 15 years.[7]

The Act relates to all aspects of the healthcare practitioner-patient relation: entering into a treatment relation which also includes diagnostic tests, informed consent for diagnostic tests or therapeutic procedures, the right to know outcomes and the exemption to that, the right not to know and the exception to that principle as well, representation of minors and incompetent patients, an aspect of medical liability, being that if a procedure is performed in a hospital the hospital will be liable for medical negligence even if the procedure was performed by a doctor who is not employed by the hospital, etc.

Relevant here is the following:

- A physician should keep a medical file, containing all relevant aspects which result from the treatment;
- The file should be kept for 15 years or as much longer as follows form the professional standard or the decision of the patient;
- Access to medical data without the consent of the patient is only allowed by those who are part of the treatment team necessary for executing the treatment contract and only insofar as necessary for their role in the treatment contract;

[4] Being the legal person where a healthcare practitioner is employed .

[5] In a famous decision concerning the transmission of hospital data to the National Health Care Authority this method was being used and the AP did not criticize this.

[6] Act of November 17, 1994, entry into force April 1995.

[7] Amendment of Act on medical treatment, December 22, 2005, Staatsblad 2006, 29

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

- Hence this also covers access for medical research. Yet, there is an exception which will be discussed in section 2.b.

The Netherlands has an Act on medical research, Wet inzake medisch wetenschappelijk onderzoek met mensen, WMO[8]. The remit of the WMO is limited. The Act on medical research involving human subjects only covers research where persons are subjected to procedures in the context of research are being asked to perform specific acts (article 1.b). Such research must first be authorised by an approved ethics committee.

Filling in a questionnaire does not fall under the scope of the WMO. Yet, if that would be asked very frequently, it might be seen as asking to performing certain acts. The same would be the case when those questions could be very distressing. Obviously there is a grey area here.

Ethics committees are often inclined to expand the remit of the Act as there is no statutory provision for ethical vetting outside this Act. 'Further use' for research of health data which have been collected in another context, such as through the treatment contract, certainly falls outside the scope of the WMO.

It should be mentioned that through self-regulation many hospitals and research institutions have established ethics committees for observational research. The lack of coordination often leads to the situation that when data come from various sources, several ethics committees must give an opinion. Sometimes opinions even conflict.

The Act on Statistics Netherlands (Wet op het Centraal Bureau voor Statistiek, Wet CBS)[9] is relevant for research as well.

Statistics Netherlands (CBS) collects many data about the Dutch healthcare and social system. It also is the holder of the death registry with the cause of death as given by the doctor.[10] The data are collected under the CRN which is replaced at CBS by an internal number. Data are combined and analysed under that internal number.

Researchers can use the data at Statistics Netherlands if sufficient measures have been taken against re-identification (article 41 Wet CBS). CBS has instituted a remote access facility for this research. If they fulfil certain requirements, researchers get access to the raw CBS data and can analyse those for their research. They can only export the results of those analyses as anonymous statistical outcomes. Not just the CBS data can be analysed in this way. Researchers can bring the raw data of their cohorts to the CBS and combine them with the CBS data. Again only anonymised may be exported in that case.

[8] Act of February 26, 1996

[9] Act of November 20, 2003 as amended since then

[10] If there is no reason to doubt about natural death being the cause, the certificate can be given by the treating physician.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Data about the cause of death can be identifiably exported to the research database of cohorts if the participant has given explicit consent to this (article 42a Wet CBS).[11]

Indirectly relevant is the Act on quality, complaints and disputes in care (Wet kwaliteit, klachten en geschillen in de zorg, Wkkgz).[12] Amongst other things this Act requires that health care providers monitor the quality of care and collect and process data in that respect in such a way that those data are comparable with those of other health care providers of the same category (article 7.2 Wkkgz).

This supposes a certain central coordination of this data processing which, however, is not provided by the Act itself. Together with other factors such as the role of health care insurers in quality control through their purchasing power[13], this had led to a plethora of national quality registries. Each quality registry covers a certain treatment area which can be more or less narrowly defined, from colon surgery in the case of colon cancer, intensive care treatment to the 'management' of patients with diabetes.

In spite of their differences they have a certain property in common which is interesting from a data protection point of view. Health care providers submitting data to a national quality registry all employ the same data processor in the sense of article 4.8 of the GDPR (or till 25-5-2018, article 1.e of the WBP). That central data processor is designated by the national coordinator of the specific registry.

Needless to say that such registries where data of participating hospitals are organised in a standardised way, are useful for research as well, even though this may be a rather limited dataset, namely based on the quality indicators of the registry. Yet, as they need to allow for case mix control (an obese patient is generally more difficult to operate than a slender one, age matters of course, etc.) they also contain many general patient data. The governance of all quality registries known to the authors of this report, allow for the release of those data for research. They usually have an advisory board set up by the coordinator of the quality registry which decides whether data may be released for research. The data can usually only be released if the data are fully anonymised. Yet, some also allow for releasing de-identified data which cannot be considered anonymous if the patient has not objected to this 'further use' and other conditions have been met. We will come back to this in paragraph 3.

A last general aspect of the Dutch system of health care data is the strong focus on data security. A ministerial Decree states that all health care providers must comply with data security norms concerning health data as issued by the Dutch Normalisation Institute (NEN). The main NEN norm is number 7510.[14] That norm is a translation of ISO 27001/2. Without certification according to that norm, health care providers are not allowed to use the CRN. In the tradition of self-regulation the representative societies of all health care in the Netherlands have drafted a model

[11] The clause also provides for a nuanced solution if the participant did not explicitly consented. However, that part was only used some years after 42a came into force in 2004. Before that time the CBS never gave the cause of death. Hence researchers never asked this in their consent forms though they did ask for consent for linking with other registries.

[12] Act of October 7, 2015

[13] It would be a too long discussion to explain the Dutch health care system. But to avoid possible misunderstandings, the following. Dutch health care insurers compete with each other, just as Dutch health care providers. However, against a very strong and strict framework of public law. The national health care insurance package is decided by public law. Health insurers cannot refuse to accept a potential insured to this package. Those already insured can change from insurers in December based on the prices insurers have made public. However that price which insured pay monthly is marginal in comparison to what the state supplements through the taxation system. There is a 'risk equalisation' running on the background which compensates insurers with 'bad risks'. This is also meant to avoid that insurers will compete for less risky insured such as students. Yet, insurers purchase health care for their insured and the idea is that they will also steer on quality.

[14] Available at NEN via https://www.nen.nl/NEN-Shop/Norm/NEN-751012017-nl.htm

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

controller-processor agreement. This model requires certification according to NEN 7510 of the data processor as well.

Though formally not applicable to data which are only used in the research context, the NEN norms have an impact on research data as well. Health care providers will not release identifiable data to a research database which does not comply with these norms or ISO 27001/2.

Many professionals in Dutch health care are regulated by the Act on professions in individual health care (Wet beroepen individuele gezondheidszorg, Wet BIG).[15] For those regulated professions the Wet BIG regulates their professional domain, disciplinary sanctions and professional secrecy (article 88 Wet BIG). Professional secrecy in general is also secured in the Penal Code (article 272).

Shared electronic health records are indirectly relevant in this context because they can potentially be an important source for health-related research.

The Netherlands does not have a national or even regional system where patient files from various health care providers are combined, with the exception of mentioned quality registries. Yet, in those registries they are only 'combined' for quality control purposes. For those purposes one sometimes has to search over the boundaries of each health care provider submitting data to the central processor, such as when the quality indicator concerns a re-operation within a certain timeframe. That re-operation might take place at another health care provider. Additionally, each health care provider will remain the controller of the data it has submitted. Potentially it can always block that release of data for research from the assembly of the data which would incorporate the data which that health care provider has submitted.

There are various systems to share data from files in the treatment context. A distinction has to be made here between 'push' and 'pull'. If data from one health care provider to another are sent by push no specific conditions regarding consent are required. If for example the patient is referred by the general practitioner to a medical specialist and the patient has agreed with this referral, the necessary data can be sent with presumed consent. The same applies to the message back from the specialist to the general practitioner. Obviously the data have to be sent in a safe way. There is another NEN (7512) which sets the general requirements for the safe digital transport of health data.

If, however, data are derived from the patient file of previous health care providers by a successive health care provider, that is considered pull and a specific regime applies. Data from patient files can be uploaded via the Netherlands Exchange Node (Landelijk Schakel Punt, LSP)[16] or by regional exchange systems. The node does not contain patient data but only metadata regarding consent and health care providers.

[15] Staatsblad 1993, no. 365, as amended since.

[16] An association of GP's, pharmacists and hospitals started the Association for Healthcare providers for Care Communications (VZVZ) in 2011. The VZVZ develops and manages the availability and access to the LSP. See: https://www.vzvz.nl/ (one has to pass an unnecessary 'cookie wall' first).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Originally the government had proposed that patient data could be exchanged via the LSP if the patient had not objected to this. All citizens were addressed with a letter about this national opt-out system. For the uploading health care provider specific conditions would apply. It should be proven that this was only done in the context of a treatment relation. However, after a long debate outside and inside parliament, the system was completely reversed.

Mentioned Wabvpz[17] states since July 2017 that the patient should have explicitly consented to a pull system (article 10a). After a transition period which will probably end in July 2020, it should be possible to make this consent granular, if the patient so wishes:

- Which type of data may be uploaded;
- Which types of health care providers or even which named health care providers may upload data.

There is not an EHR (electronic health care record) system which can support this granular consent at the moment and hence the transition period.

The conclusion is that the Netherlands has a sort of decentralised national patient record via the LSP. Yet this has only been developed in the context of treatment (for example the pharmacy can have access to laboratory data to correct the dosage of a drug) and research has been explicitly left out of scope, the discussion being sufficiently complicated already for the primary purpose. Additionally it is fully dependent on patient consent. Thus far only about 15 % of the population has opted in for exchange via the LSP.

b. Revision of the current legal framework under the GDPR

How are the necessary changes to the national data protection framework introduced by the GDPR addressed in your country? What is the adopted legislative approach?

In December 2017 the government submitted the Bill on the implementation of the GDPR to the Second Chamber of parliament.[18] . In Dutch: the Uitvoeringswet Algemene Verordening Gegevensbescherming , UAVG . The Bill was accompanied by a letter from the minister of Justice and Security pleading to have a speedily parliamentary proceeding. That plea was successful. The Bill was accepted by the Second Chamber in April 2018 and, without discussion, by the First Chamber of Parliament on May 15 2018. The UAVG will enter into force from May 24 onwards.

The UAVG does not repeat what is in the GDPR already. The UAVG only offers provisions where the member states have leeway, hence most of all on the context of articles 9.2 GDPR and 89.2 GDPR. In accompanying explanation to the Bill by the government stressed that the Bill did not change anything compared to the WBP in this respect.

Additionally the UAVG institutes the AP as a Data Protection Authority in the sense of article 51 of the GDPR. Also here the UAVG does not repeat what is in the GDPR already. Most provisions about the AP relate to linking article

[17] See footnote 2

[18] Parliamentary Proceedings under number 34851.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

51 and following of the GDPR with the Dutch regulations on investigative powers of administrative authorities (in the General Act on Administrative Law, Algemene wet bestuursrecht, Awb)[19] and the special Act on independent administrative authorities (Kaderwet zelfstandige bestuursorganen, Kaderwet ZBO)[20]. According to the provisions of latter Act, such authorities cannot be too independent but are in general subject to ordinances of a minister which is responsible for the field of application of such authorities. Given the independence of a Data Protection Agency several exemptions had to made to the Kadetwet ZBO.

As the UAVG is only filling in caps for the Dutch situation, the UAVG is fairly concise. It only has 54 articles.

The UAVG also contains a clause which makes the GDPR applicable to purely internal (hence without any potential cross-border effect) data processing, such for a small local club which organises card games and does even have a website (article 3.1.b).

The parliamentary proceedings to Bill clearly state that there was no intention to change anything which did not need to be changed. Hence the regime for using health (care) data for research did not change. The regime is the same as under the WBP and WGBO.

c. The national data processing authority

Can you provide a short description of the role of the data protection supervisory authority in your country in the domain of processing health data for research purposes under the current legal framework?

The AP is an independent administrative authority under Dutch law. It was instituted under the WBP and till 2016 called het College Bescherming Persoonsgegevens.[21] It has a role in advising government on new regulations and overseeing compliance with the WBP and now the GDPR and UAVG. It's members are appointed by the Minister of Justice and Security after a recommendation by the Crown.[22]

Its budget is determined by the Minister of Justice and Security based on a budget proposal of the AP.

The WBP contains few instances where a proposed data processing had to be approved by the CBP/AP first. Processing health data or processing data for research was not one of them.

Obviously there a controller needed to notify to the CBP and later the AP about processing of personal data as that followed from Directive 95/46/EC. Notification was a mere formality and with the advent of the GDPR the AP did not actively follow-up on the absence thereof in its compliance policies. A Royal Decree stated when notification is

[19] Act of June 4, 1992

[20] Act of November 2, 2006

[21] The amendment of the Wbp with the notification porcedure for data breaches also changed the name of the CBP into AP.

[22] Which means the whole government. The same procedure applies to judges in the High Court and the Council of State.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

not necessary. In case of data processing for research if the data would be de-identified within 6 months after the start of the research.

Can you describe the adopted or proposed changes to this role of the national data protection authority to ensure compliance with the GDPR?

As mentioned, the UAVG only changed the existing regime to align with the GDPR and Dutch provisions of administrative law. Everything which is in the GDPR already about a national DPA is not repeated in the UAVG but the UAVG gives rules about how this should be done. Dutch administrative authorities are not as such competent to cooperate with other authorities unless Dutch law would explicitly allow that. As all DPA's should cooperate in the European Data Protection Board and with each other in case of complaints, the UAVG explicitly allows this (article 19).

Codes of conduct and certification are already regulated under the GDPR hence the – while the WBP had a clause about the approval of Codes of conduct (article 25 WBP) - the UAVG is silent about this issue, except for the kind of administrative procedure which should be followed to approve a submitted code of conduct (article 14.2).

The one example where a kind of processing had first to be submitted to the AP has been deleted as the GDPR is supposed to regulated this exhaustively (in section 3 of the GDPR).

Obviously the notification procedure has been abolished as that was supposed to one of the advantages of the GDPR with the internal 'records of processing activities' (article 30) coming instead thereof.

2. Transposition of Article 8.4 of Directive 95/46

Did your national legislator insert any additional exemptions for the processing of health data for research purposes? How is it/are they formulated? Please explain. Are there additional exemptions issued by the DPA?

Art. 8.4 of Directive 95/46: "4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority."

a. Transposition of Article 8.4 of Directive 95/46

As mentioned the Dutch transposed the Directive as closely as possible. Hence in the WBP data concerning health became a special category of personal data and as such its processing would be prohibited unless one the exemptions would apply (article 16 WBP). The first one them would be the express consent of the data subject (23.1a). There was also an exemption in the context of research, (article 23.2) when:

a. the request of specific consent proves impossible or would demand unreasonable effort;

b. the research cannot be executed without those data

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

c. the research serves a general interest;

d. the execution is covered by such guarantees that the personal life of the individuals involved is not unreasonably harmed.

Not following from the transposition of the Directive but since 1995 already part of the WGBO was the clause that releasing patient data from the 'treatment team' to a researcher without explicit consent (which is the default situation) is also possible if (article 7:458 BW):

1: …….

a. the request for consent is not reasonably possible and the execution of the research is covered by such guarantees the personal life of the patient is not unreasonably harmed, or

b. the request for consent, bearing in mind the nature and the aim of the research, cannot reasonably be demanded and the health care provider has made sure the data is made available in such a form that re-identification of individual patients is reasonably pre-empted.

2. Provision of data in accordance with paragraph 1 is only possible if:

a. the research serves a general interest,

b. the research cannot be carried out without the data concerned, and

c. as long as the patient involved has not specifically objected to such provision of data.

3. Such provision of data in accordance with paragraph 1 is duly noted in the patient record.

That is all. For all the rest, the general regime would apply. It should be noted that section 1b of 7:458 BW does not refer to anonymised data. Anonymised data can always be released.[23] The section refers to data which have been de-identified.

In the Dutch tradition of self- or coregulation[24] Dutch researchers for observational health research drafted a Code of Conduct which was approved by the then CBP in 2004.[25],[26] It already had many 'privacy by design' and data minimisation aspects which are now in the GDPR. Regarding mentioned article of the WGBO it stated that it was not sufficient that data would be de-identified before leaving the health care provider but also at the research side there should be sufficient technical and administrative procedures that the patient would not be re-identified.

[23] As they fall outside the scope of data protection legislation. Though it is a different question who may perform such anonymisation. Those should have legitimate ground for access in the first place. The ICT department may perform this as that already has 'access' to maintain the EHR system for treatment purposes.

[24] See about this tradition D.D. Hirsch, Going dutch? Collaborative dutch privacy regulation and the lessons it holds for U.S. privacy law, 2013 MICH. ST. L. REV. 83.

[25] Staatscourant 2004, no. 82.

[26] The text can be found at: https://www.federa.org/sites/default/files/bijlagen/coreon/code_of_conduct_for_medical_research_1.pdf

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The Code of Conduct also contained detailed recommendations about how the opt-out system of 7:458 BW should be implemented before a researcher could rely on it.

Though the approval of the CBP of this Code of Conduct has long been expired, ethics committees and funding agencies still refer to it when approving research.

b. The regime applying to the processing of personal data for health research purposes

Is there a specific regime applying to data processing for research in the field of health purposes?

Except for data which are assembled in the context of WMO research, there is no other regime than that explained supra ad A. And actually the WMO does not have specific rules either. The data should be pseudonymised before they leave the treating physician. Yet, that does not follow from Dutch data protection law but from the clinical research guidelines, such as the GCP.

From which generally applicable data protection provisions are researchers exempted and under what conditions?

Under specific conditions as explained in A supra, a researcher may process sensitive data without explicit consent.

Additionally, the duty of notification (that one processes personal data) does not apply to research which is done in institutions for research. Neither does the duty to give an overview upon request which data are being processed (article 44 WBP).

c. Are there additional specific conditions governing the processing of data for scientific research purposes?

What are the suitable safeguards applied to the exemption foreseen by Article 8.4 of the Directive in your country?

As seen in section A infra, the law uses rather broad terms in this respect. There are no Ministerial of Royal Degrees or recommendations of the CBP/AP which narrow these down, except for a general guideline of the then CBP on data safety. In the context of health data that guideline has been superseded by the much more detailed NEN norms.

I should be mentioned that the 2004 Code of Conduct did give more detailed provisions. Next to those already mentioned, the Code of Conduct also states that research should be based on a research protocol which amongst

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

other things should explain the reasons behind the research and why the requested data are necessary to perform the research.

Are there any specific provisions concerning: (i) professional secrecy, (ii) express consent for specific data, or specific provisions for (iii) deceased data subjects, or (iv) specific provisions for minors or persons subject to guardianship?

The answer here will not repeat what has been discussed already. Hence, only the following issues remain:

- There are specific provisions in the law for professional secrecy of health care professionals (see supra) but not for researchers. Yet, in addition to mentioned Code of Conduct, all labour contracts of research institutions explicitly refer to secrecy concerning personal data which they have encountered in their professional capacity.

- As discussed, there is a nuanced system as follows from Directive 95/46/EC. There is no provision in Dutch law which states that personal data, even sensitive data, may only and without exception be processed with explicit consent. There will always be some sort of exception, yet, very much depending on the circumstances.

- The WBP/UAVG does not apply to deceased persons. The WGBO however does. In that situation one would not be able to ask for consent in the sense of 7:458 BW.

- The regime for minors under the WGBO and the WBP/UAVG differs. Under the WGBO minors from 12 years onwards have their own right to privacy. Hence, they should consent as well, next to their legal guardians (in general the parents). Under the WBP/UAVG the right to privacy starts at 16. Before that age they are fully represented by their legal guardians.

- In the case of incompetent persons there is a distinction between the WGBO and WBP/UAVG as well. An incompetent patient under the WGBO is a patient who cannot make the relevant decisions at the time when those are necessary in the treatment context. They are then represented, except emergency situations where the physician can make decisions in the best interests of the patient. The representative can also be a representative which has not been nominated by a Court such as a family member (7:465.3 BW). Under the WBP/UAVG only persons who by a Court order have been declared incapacitated will not be able to make such consent decisions and hence should be represented by the guardian which has been appointed by the Court. In the Netherlands there are three regimes for persons which are fully or partially incapacitated. If the incapacity would only apply to financial affairs (in Dutch 'bewindvoering') that person could still consent to participate in research or 'further use' of his or her data for research.

Are there specific requirements about the data subject's information or about the person from whom the data was collected?

The requirements for research are the same as for data protection in general. Yet, as also follows from the Code of Conduct, the bar has been raised higher if data subjects are specifically asked for consent. In that case the research should be clearly explained and also the data procession attached to it .

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Yet, under the pre-GDPR regime, such consent could have been broad consent and the detailed privacy declarations as prescribed by article 13 GDPR were not deemed necessary.

If the researcher would receive personal data from a third party, mentioned article 44 of the WBP would apply. Additionally, the Code of Conduct, requires that such data should be de-identified as much as possible. In GDPR terms article 11 would apply to such data.

Are there specific penalties if the conditions for processing for scientific research in the field of health purposes are not respected? What do those penalties entail?

No if the question is meant to ask for penalties specifically for research. Research falls under the general regime including the data breach notification and penalties for not adhering to security standards for processing (sensitive) personal data.

d. Formalities prior to processing: the general regime under the current framework

Is there a regime requiring the fulfilment of certain conditions prior to any processing activities different from that applicable to research in the field of health? If yes, what does that regime entail?

No. From co-regulation it follows that most research will be vetted by an ethics committee following either internal rules of the database which releases the data or the researcher which receives them.

3. Further processing of health data (for research purposes): the current regime

How is the notion of further processing regulated in your national framework?

In article 9 of the WBP the Directive was transposed. Further processing for research or statistical purposes was not considered incompatible. For other purposes the compatibility test had to be performed. This is not test which they controller did have to submit for approval to the CBP/AP. In its ad hoc compliance review (usually after a complaint) the AP could state that it considered the further processing not compatible.

Are there specific conditions to the further processing for scientific research in the field of health purposes?

As mentioned, 'further use' of health data for research is not deemed to be incompatible with the original purpose. Yet, the rules of the WGBO would still apply regarding who can have access to such data. Hence only those whose involvement is necessary to execute the treatment relation should be involved in the 'further use'. But that can be

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

a broad category, subject to the roles and rights matrix which follows from mentioned NEN Norm 7510. ICT employees have rather general roles to keep the EHR system running. They can be involved in this further processing as well, especially when that involves anonymisation of the data.

What are the rights of the data subject when it comes to further processing?

This is very general question which must be answered in a nuanced way. The answer is limited to further processing and does not discuss data subjects rights in general.

The data subjects do not have specific rights insofar as the data are further processed for research or statistics by the same controller, such as a health care provider. The legal basis does not change. However, as follows from the previous section this would only apply to those how may have access to the EHR already.

If further processing would be done for other purposes, the controller should meet the compatibility test. If the controller would not meet those criteria, consent would be needed, in the case of sensitive data, explicit consent.

If personal data based on further processing would be transferred to a researcher, even within the same controller, that researcher would obviously need a new legal basis. Which can only be explicit consent or the research exemption discussed earlier.

As one of the conditions to release data from a health care provider to a researcher under that research exemption of the WGBO is the absence of a general objection to research with personal data outside those involved in the treatment relation already, it is difficult to apply the research exemption to critical care and ICU research (unless ICU is the result of a planned operation).

The need for a research exemption to release data would not apply to data which have been anonymised. Those fall outside the scope of data protection legislation and hence do not need a legal basis. The AP

Yet, it is difficult to explain that one can object to research with data which are de-identified and processed under conditions where re-identification is very unlikely to occur and not to data which are anonymous. This difference will escape most patients.

What about the data subject's rights and further processing for scientific research purposes?

See the answer to the previous question.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

4. The GDPR's impact on the current regulatory framework for the processing of health data for research purposes

a. The impact of the GDPR on the rules applying to processing for research in the field of health

Please provide a summary of the main relevant characteristics of the new law/Bill (as far as it is relevant for processing health data for research purposes). How is (or will be) Article 9(2)(j) implemented in your country?

As mentioned already, the intention of the UAVG was to change as little as possible compared to the WBP. Hence mentioned article 23.2 WBP as the broad research exception was left intact (with some minor changes in the wording). It is now article 24 UAVG.

Following the GDPR which recognises genetic data as a special category of sensitive data, a new clause on genetic data was inserted in the UAVG (article 28). Also this article has the research exception to the consent principle as discussed earlier.

The parliamentary papers accompanying the UAVG Bill explicitly stated that article 7:458 BW, (discussed supra), is still valid, although dating from 1995.

The UAVG also implements article 89.2 GDPR. Article 44 UAVG states that:

If the processing is performed by institutions or services for scientific research or statistics, and there are sufficient guarantees that the personal data will only be used for these purposes, the controller may abstain from the application of articles 15[27],16[28] and 18[29] of the GDPR.

The parliamentary papers argued that the government choose not to exempt the application of article 21 GDPR in the context of research (as would be possible under 89.2 GDPR).

Hence there will be the opportunity to object if the data processing for research is based on points e and f of article 6.1 GDPR. A health care provider does not process patient data on that basis but based on point c of 6.1. The WGBO requires that patient data are collected and recorded in the medical file, now the EHR. Hence, as further processing pursuant to article 5.1.b GDPR, does not affect the legal basis, the opt-out system does not apply to such 'further use' of patient data as such. It would apply to researchers as receivers of the data (insofar as article 11 would not apply). However, also article 21 has a research exemption which applies directly, see 21.6.

[27] The right of access

[28] The right to rectification

[29] The right to restriction of processing

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

In 21.6 of the GDPR is the phrase 'pubic interest' used as on many other occasions in the GDPR. We have seen that this phrase is also used in the Dutch research exemptions (24 UAVG and 7:458 BW). There is no authority designated which may decide which research is the public interest and which is not. Neither is there any jurisprudence.

The Code of Conduct makes an attempt by stating that any health research which adheres to good research practices and scientific integrity is in principle in the public interest as it increases public knowledge which can help to improve health care and the health care system. Additionally, ethics committees should vet research. As seen, both are based on self-regulation.

b. Modification to the processing authorisation procedure applying to research in the field of health

There is not an authorisation procedure under the WBP and no modification of the absence thereof based on the UAVG. The rather liberal system with self-assessment and the lack of prior authorisation from the AP or another governmental body remains the same.

As from May 25 2018 the self-assessment must be supplemented with the data protection impact assessment of section 3 of the GDPR. As that is already completely regulated in the GDPR, the UAVG does not mention it. It remains to be seen what will happen if the result of a DPIA would be submitted to the AP pursuant to article 36 GDPR. The AP has in general not been known for being a very responsive organisation.

How will the processing authorisation procedure (if any exists) be affected by the implementation of the GDPR? Can you describe any such change?

There is no prior authorisation procedure under the pre-GDPR law and as follows from the previous section, no changes will be made. Hence there is no effect except those which follow directly form the GDPR. Those are obviously not specific for the Dutch situation.

What about the right of the data subject and the obligations of the controller?

The specific clauses regarding research have been discussed in section A of this paragraph already.

For the rest the GDPR would apply. If the research would rely on explicit consent then article 7 would apply with the possible mitigation of Recital 33. There should be the notification of article 13 the GDPR etc. In that sense the bar will be set higher. Those are general GDPR aspects and not specific for the Dutch situation.

5. Further processing for research purposes under the GDPR

The notion of further processing under the GDPR:

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Article 9 of the WBP has been abolished in the UAVG as this issue has been regulated in the directly applicable GDPR articles 5.1.b and 6.4. As mentioned already, the UAVG refrains from repeating the GDPR, even in the same wording.

The meaning of the further processing for research has been explained already and nothing is expected to change in this respect.

How to measure the compatibility of purpose of the further processing:

Article 5.1.b and 6.4 of the GDPR give the guidelines. Those are not supplemented by Dutch law or ordinances/recommendations of the AP.

Perhaps it should be mentioned that further processing of patient data for quality control and transparency about the quality of health care providers is generally not seen as further processing in the sense of article 6.4 GDPR but inherent to providing health care which should always be of good quality (see mentioned Wkkgz).

The particularities of scientific research: a presumption of purpose compatibility

It has been mentioned already that this presumption which was already in the Directive and hence in the implementing WBP. As argued, now it is in the GDPR and directly applicable.

Given the regime applied to further processing in the GDPR, can you describe the consequences, if any, in your national legal framework?

These consequences, or better the lack thereof, have been discussed already.

6. Health data sources for research purposes

a. Sources of data and their regulation

Does your national framework contain specific provisions for anonymised or pseudonymised health data?

The national regime does not contain provisions for anonymised data as those fall outside the scope of data protection legislation. Neither does the national framework contains provisions on anonymisation.

It should be mentioned that the AP just as the Article 29 Working Party, still refers to the Article 29 Working Party paper on anonymisation techniques of 2014 even though that view has been substantially nuanced by the Breyer judgement of the CJEU of October 2016.

Pseudonymisation has gotten a distinct meaning in the GDPR. They are personal data with a specific property (article 4.5).

In the Netherlands pseudonymisation has been used in a different meaning. It meant replacing the direct identifiers by a one way hash through a Trusted Third Party and releasing research data under that pseudonym which were not indirectly identifiable (according to the Breyer standard).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Those data could still be considered anonymous data.[30] Yet, there is substantial confusion about the subject. Perhaps the latter procedure should use a different name.

What are the different sources of health data that can be used for research purposes?

- **DIRECT COLLECTION FROM PATIENTS:**

Under the current legal framework: please explain the currently applying rules that a researcher, who intends to collect health data directly from individuals (e.g. via a survey, or by asking patients to wear a monitoring device, etc.), should follow.

There are no specific national rules for starting such a new project, assuming that it would not fall under the ambit of the WMO.

In most instances the researcher would need the approval of the ethics committee of the institution where he or she is employed. That committee would request that the Code of Conduct is followed.

Obviously explicit consent would be needed with a participant information leaflet explaining the research. The data safety of the monitoring device should be assured.

If the participants would be recruited via health care providers, those health care providers should send the invitation with enclosed a letter of the researcher. As obviously the researcher is not allowed to have access to patient data at this stage, including not to their names and addresses. It is accepted that a data processor (then acting as a 'mailing house') may be employed for this purpose.

Potential participants could also be recruited via municipalities. The 'Act basic registration persons' but less literally and more aptly translated as the Act on civic records (Wet basisregistratie personen)[31] allows that researchers can receive basic data for recruitment of participants for research if the citizen has not opted out to this.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

The national rules will not change. The GDPR will add additional requirements. Dutch co-regulation already required that the information in the context of research was quite elaborate, yet it remains to be seen whether more broad consent is still feasible. The list of article 13 must be met and in general a DPIA must be executed. Dutch research institutions are developing a sort if 'mini-DPIA' for research which is similar (see article 35.1 GDPR last sentence) to research for which a DPIA has been executed already

[30] For a view of the author of this report see: http://www.medlaw.nl/publicaties/anoniem-gecodeerd-gepseudonimiseerd-hoe-zit-het-nu/ . See also recently for a similar view: Mourby et al., *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK,* Computer Law & Security Review 34 (2018) 222–233.

[31] Staatsblad 2013, no. 316, entry ito force 01-07-2014 as amended since.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

- **COLLECTION FROM HEALTH PROFESSIONALS AND HEALTH INSTITUTIONS**

Under the current legal framework: please explain the rules currently applying that a researcher, who intends to obtain health data from medical staff, hospitals, etc., should follow.

This very much depends upon the scenario and applying the rules and principles discussed earlier to that scenario or 'use case'.

If the researcher would only request anonymous data, there would be no legal hindrances. Yet, the health care provider is under no obligation to cooperate.

If the researcher would request personal data, informed consent would be necessary or the research exemption of 7:458 BW could apply. It seems as if health care providers have become more reluctant to release personal data under the latter clause.

Here we also encounter a side effect of the rather liberal Dutch regime of self-regulation. The researcher should submit the approval of his or her ethics committee but also the ethics committees of all the health care providers which are addressed by the researcher will probably need to be heard. This can lead to divergent conclusions as has happened in the past already.

Under the revised legal framework: Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

As argued, nothing changes with respect to Dutch law.

- **PRIVATE DATABASES**

Under the current legal framework: please explain the rules currently applying for the setting up of and the use of a private database with health data for research purposes.

There are no specific rules. A database is not considered different than the research project as explained earlier. Obviously all research results in a database. The Code of Conduct mentioned that the data should be anonymised as soon as they were not necessary for the project anymore, which also included for validation purposes. The recent application of the FAIR principles to which researchers should adhere, will change this yet it is unclear how the balance will be struck.

It should be mentioned that there are far more private databases than public databases, though many of those private databases receive public funding. An overview can be found at:

https://www.volksgezondheidenzorg.info/zorggegevens. Also the quality registries are listed there.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Major examples of such databases are the Dutch National Cancer Registry[32] and NIVEL primary care database.[33] These two are based on the research exemption of 7:458 BW and 23.2 WBP (24 UAVG form May 25 2018 onwards). Each private database has its own governance regarding releasing data for research. Sometimes the data controller will require that project submitted by the researcher will become a common project.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

As mentioned the legal basis or procedures will not change.

- **PUBLIC DATABASES**

Under the current legal framework: do public authorities make available health data for research purposes in your country and under what conditions?

Some databases are kept by public authorities. Either because they are based on the law or because they are instituted by a public authority such by the RIVM, the Dutch National Institute for Health and the Environment.

It is a diverse landscape.

The data kept by CBS (Statistics Netherlands) have been discussed already.

The other public database instituted by law is the database of diagnostic codes and their costs as submitted by health care providers which is kept by the NZa, (Nederlandse Zorgautoriteit, Dutch Healthcare Authority). These data are primarily gathered to steer the health care system, hence for policy purposes. Some of the aggregated data are published as 'open data'.[34] There is not a provision in the governance of the database which would give researchers access to more detailed data.

Regarding the RIVM databases it very much depends on how the data were collected. With some of these databases the RIVM is the mere data processor for the submitting health care providers. This is the case for the database with sexually transmitted diseases. Other databases are based on data which the RIVM has collected itself in the course of its activities. This is the case for data about the national vaccination program. And there is much in between.

There is not a special law which allows the RIVM to collect data making an exception on the general data protection regime. This with the exception of notifiable infectious diseases but that is in all EU member states always an exception, pursuant to the WHO Treaty of the International Health Regulations.

The RIVM will need to use the general regime of data protection including at times the research exception. Whether that has been the case depends on each database. Hence, each has its own governance. It is impossible to give a statement about further processing by researchers outside the RIVM which is applicable to all.

[32] https://www.iknl.nl/over-iknl/about-iknl

[33] https://www.nivel.nl/nl/nzr/zorgregistraties-eerstelijn

[34] http://www.opendisdata.nl/dis/over

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

No. Yet there is some discussion whether the Act on the RIVM shouldn't be changed to give the RIVM a more special status to process health data without explicit consent.

b. Application of the national framework to the AEGLE cases

In the AEGLE project, the "research objective is to establish the use of Big data analysis in the prediction of outcomes in three working scenarios: Chronic Lymphotic Leukemia (CLL), Intensive Care Units and type 2 diabetes for the prediction of adverse outcomes. The research methodology is Big Data analysis to establish predictive values that may apply in three clinical scenarios and to see if this can be generalised to other healthcare disease models". [35]

To achieve its objective, the AEGLE project must base its approach on the study, and thus the processing, of data concerning health. This section aims to address each of the three proposed AEGLE cases, and to determine the requirements in general terms for access and the processes relevant to data under the Directive (the current framework) and the GDPR.

The questions will be answered both regarding the pre GDPR situation as for the after GDPR situation as, as argued, nothing changes fundamentally

1. Type 2 diabetes

The AEGLE project uses, after pseudonymisation, existing databases with health data collected from patients who expressed their consent to their data being used for research purposes.

The are no such databases in the Netherlands. The NIVEL primary care database might have such patients. Yet, as seen, data there are not based on consent.

The same applies to the Diabetes Quality Registration. That is a registration about diabetes care and management in hospitals, including University Medical Centres. While the NIVEL database has pseudonymised detailed personal data, the Diabetes quality registration only has data needed for quality control and benchmarking. But as argued these can be detailed as well insofar as necessary for case mix control.

The governance of both databases explicitly allows that the data may be used for research. Yet, their legal bases differ and hence how this can be done. NIVEL is the data controller of the primary care database. Given the pseudonymisation, which is very strict, article 11 GDPR applies to this database.

With the diabetes quality registration all participating hospitals remain controllers of the data. They have mandated a national coordinator of the registry to make certain decisions on behalf of them but can always revoke that decision.

[35] AEGLE Grant Agreement, Annex 1, p. 83.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

There will be strict requirements about which kind of data can be released. In the case of NIVEL, the project could be set up as a common research project in which case, by using the NIVEL research platform, more detailed analyses and even linking to other databases would be possible. The NIVEL privacy committee should approve the project. In the case of the diabetes quality registry the privacy committee of that project should approve. Only anonymised data will be released.

Yet, in both cases Eagle should give up the idea that this further processing is based on explicit consent if it wants to use the data as they are in those database. Of course, there could be a new project where patients are invited to participate and which (also) makes use of the data which are in one of the two databases (or both) already. That would need the cooperation of all health care providers which should recruit those patients and of the NIVEL and/or the coordinator of the diabetes quality registry.

2. Intensive Care Unit (ICU)

AEGLE uses data generated by ICU devices without collecting the patient's consent (after pseudonymisation).

As seen, the research exemption for releasing patient data without consent depends, together with other factors, upon the fact that the patient did not object (7:458 BW). Such an opt-out system is only feasible for planned operations with need the ICU in the first post-operative period but not for the majority of the patients. Hence only anonymous data can be released.

Those could be one-way pseudonymised and still be anonymous data. See the discussion at p. 16.

The national quality registration for ICU's is called NICE.[36] Being a quality registration, it might not have all the necessary data. NICE releases data for research. These would be fully anonymous. In theory it would be possible to have more nuanced analyses being performed in the registration itself by the data management of NICE. The data processor for all participating hospitals in NICE is the department of medical statistics of the Amsterdam Medical Centre.

3. Chronic Lymphocytic Leukaemia (CLL)

The AEGLE project re-uses, after pseudonymisation, data coming from biobanks. In this instance, patients have given their informed consent for the samples and for the processing of their data. But this consent was given in general terms and not specifically for AEGLE.

I understand that Eagle does not request samples but data coming from the analyses of the samples. The question is unclear whether new analyses need to performed to answer the request or that already existing analyses of the biobank are sufficient. Perhaps that will depend on what data the biobank has already

[36] https://www.stichting-nice.nl/

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The governance of all Dutch biobanks differs though all are based on another piece of Dutch co-regulation, the Code of Conduct on proper use of tissue for research which dates from 2011.[37]

The biobank which could be used in this respect, would be the "Pearl" 'leukemia, myeloma and lymphom'a of the Parelsnoer Institute, a collaborative effort of all Dutch University Medical Centres (PSI). [38] The informed consent of PSI is rather broad but not as broad as in some other biobanks and clearly states that data may be shared with outside researchers. Those may even involve pseudonymised personal data if certain conditions are met such as agreeing upon a data transfer agreement. The project should first be approved by the board of the 'Pearl' and at least one ethics committee of the participating centres.

As follows from the Dutch regime there is no need for prior consultation or approval of governmental body or the AP.

[37] https://www.federa.org/code-goed-gebruik

[38] https://parelsnoer.org/page/en/Home

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU