General data protection regulation – GDPR

« Algemene verordening gegevensbescherming »

Prof. Dr. Patrick Cras
Afdeling Neurologie, Ethisch Comité
UZ Antwerpen

Implications for research

Universiteit Antwerpen

Have you noticed all these mails asking for a consent for further data processing?

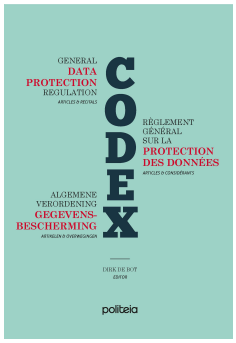
GDPR is an excellent opportunity to get rid of 90% of your spam mail…

Biomedical research and GDPR

- Medical research and legislation landscape changing due to developments in information technology
- Data driven research does and will continue to significantly improve human health
- Concern about effectiveness of existing data protection
- Need for a more consistent and comprehensive protection
- Data Protection Directive 95/46/EC (DPD) to be replaced by the General Data Protection Regulation (GDPR)
- Limits to the use of sensitive personal data
- 'consent or anonymise approach' and 'research exemptions'

Sethi 2013; Mostert, 2016; Chassang, 2017

Sources



The General Data Protection Regulation (EU) 2016/679 http://eur-lex.europa.eu/legal-content/ en/TXT/?uri=CELEX%3A32016R0679

GDPR-GEDRAGSCODE VOOR ZORGVOORZIENINGEN – ICURO 1 dec 2017

Vocabulary of GDPR

- Personal data ('persoonsgegevens')
- Controller ('verwerkingsverantwoordelijke'): determines the purposes, conditions and means of the processing of personal data
- Processor ('verwerker'): processes personal data on behalf of the controller
- Data protection officer (DPO) ('Functionaris voor gegevensbescherming')
- Data protection authority ('Gegevensbeschermingsautoriteit')
- Legitimate interest ('rechtmatig belang')

Basic principles

6 main GDPR principles

1. Processing should be lawful, fair and transparent to the data subject (**lawfulness, fairness and transparency**)
2. Collection for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Data should be adequate, relevant and limited to what is necessary for the processing purpose (**data minimisation**)
4. Data should be accurate, kept up to date and inaccurate data should be erased or rectified without delay (**accuracy**)
5. Data should be kept for no longer than necessary to fulfil the purpose, with some exceptions for archiving and research (**storage limitation**)
6. Data should be kept secure and protecting against accidental or illegal loss or access (**integrity and confidentiality**).

Beginselen verwerking van persoonsgegevens (Art. 5)

Rechtmatig, behoorlijk en transparant	Doelbinding	Data-minimalisatie
Juistheid	Opslag-beperking	Integriteit en vertrouwelijkheid
Verantwoordingsplicht ("accountability")		

6 permitted grounds for processing personal data

1. data subject has given **consent** to the processing of his or her personal data for one or more specific purposes
2. processing is **necessary for the performance** of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
3. processing is **necessary for compliance with a legal obligation** to which the controller is subject
4. processing is **necessary in order to protect the vital interests of the data subject** or of another natural person
5. processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller
6. processing is necessary for the purposes of the **legitimate interests pursued by the controller** or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject

6 permitted grounds for processing personal data

1. data subject has given **consent** to the processing of his or her personal data for one or more specific purposes
2. processing is **necessary for the performance** of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
3. processing is **necessary for compliance with a legal obligation** to which the controller is subject
4. processing is **necessary in order to protect the vital interests of the data subject** or of another natural person
5. processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller
6. processing is necessary for the purposes of the **legitimate interests pursued by the controller** or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject

6 permitted grounds for processing personal data

1. data subject has given **consent** to the processing of his or her personal data for one or more specific purposes
2. processing is **necessary for the performance** of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
3. processing is **necessary for compliance with a legal obligation** to which the controller is subject
4. processing is **necessary in order to protect the vital interests of the data subject** or of another natural person
5. processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller
6. processing is necessary for the purposes of the **legitimate interests pursued by the controller** or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject

Rights of data subjects

a) **The right to be informed**: Data subjects have the right to be told about who will be processing their data and for what reasons.

b) **The right of access**: As with the existing legislation, data subjects have the right to access their personal data.

c) **The right to rectification**: Data subjects are entitled to have personal data rectified if it is inaccurate or incomplete.

d) **The right to erasure**: Also referred to as 'the right to be forgotten', individuals may request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Rights of data subjects

e) **The right to restrict processing**: As under existing rules, individuals have a right to 'block' or suppress processing of personal data.

f) **The right to data portability:** Data subjects are entitled to obtain and reuse their personal data for their own purposes across different services.

g) **The right to object:** Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling), and
- processing for purposes of scientific/ historical research and statistics

h) Rights in relation to **automated decision making and profiling**

"All health care data are classed as special category data, commanding a higher level of protection and care."

Processing sensitive personal data

GDPR forbids a controller from processing "special categories of data" – sensitive data revealing racial or ethnic origin, religious or political beliefs, as well as genetic, biometric, and health data – except in certain enumerated circumstances, such as where the data subject provides "explicit consent" or where the data that was "manifestly made public by the data subject" (Article 9(2)(a); Article 9(2)(e)).

Essential elements of compliance

1. technical and organizational measures: internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal policies
2. maintain relevant documentation on processing activities
3. providers that carry out large scale processing of special categories of data should appoint a Data Protection Officer (DPO)
4. implement measures that meet the principles of data protection by design and data protection by default
   Data minimization
   Pseudonymisation
   Transparency
5. monitor processing, creating and improving security features on an ongoing basis.
6. data protection impact assessments where appropriate

Research in the regulation

Research in GDPR – general principles

- Research occupies a privileged position within the Regulation
- "broad" definition of research, encompassing the activities of public and private entities alike (Recital 159)
- 'data analytics' activities of many organizations may qualify as 'research'
- unclear exactly how far the GDPR's research exemption will extend
- GDPR aims to encourage innovation, as long as organizations implement the appropriate safeguards

Broad definition of research

- Recital 159 supplies examples, such as "technological development and demonstration, fundamental research, applied research, and privately funded research," as well as public health research
- Article 179(1) of the Treaty promotes "the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely."
- Requirement that research be published or otherwise made available

Research in the regulation

- Even if a controller has a legitimate interest in research, it may be "overridden" by the data subject's rights.
- Public entity may process personal data without consent under Article 6(e) – "the performance of a task carried out in the public interest" – which requires a legislative mandate from the Member State or the EU for the processing operation.

Ethical standards for scientific research

"specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes" (Recital 159).

Although not expressly stated, these "specific conditions" may refer to "recognized ethical standards for scientific research," which are discussed in Recital 33, as well as the safeguards outlined in Article 89.

Prospective collection of data for research

Informed consent strenghtened

- Plain language
- Affirmative act
- Documentation
- Witdrawal of consent
- Invalid consent
- Consent for use of minor's data
- Consent for special categories of data
- Limitations on data collection and processing: principles of data minimalization and restriction in secondary use and retention

Informed consent strenghtened

- Artt. 4(11); 6(1) (a); 7). Specific consent, namely 'for one or more specific purposes' (Art. 6(1) (a)), could pose a challenge for research
- 'it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection'(recital 33)

Art. 89 Archiving purposes in the public interest, scientific, historical research or statistical purposes

- Shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject
- Measures may include pseudonymisation or anonymisation
- Technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation
- Union or Member State law may provide for derogations
- Such rights are likely to render impossible or seriously impair the achievement of specific purposes

Pseudonymization

- is "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual" (Article 4(3b))
- Pseudonymization is not always required but rather its use is encouraged "as long as [the research purposes] can be fulfilled in this manner" (Article 89(1))

Anonymization

- Anonymous data fall outside the scope of the Regulation
- Determining whether data is anonymous is a fact-specific inquiry: when it cannot be identified by any means "reasonably likely to be used ... either by the controller or by another person" (Recital 26).
- Thus, even if a researcher no longer has the ability to re-identify a data set, such data set may still be regulated under the GDPR if it could be re-identified with reasonable effort.

Legitimate interest

Legitimate interests

- Has not changed from the 1995 data protection Directive
- Controller balances its own (or a third party's) legitimate interests against the interests or fundamental rights and freedoms of the data subject
- Unless the data subject's rights override the controller's rights, it can proceed with the processing
- Provided consent, Article 6(4) allows to process the data for a secondary research purpose
- Controller has to inform the individual (under Article 13) that it is using a legitimate interests ground for the processing

Research as a legitimate interest

- Controllers should take into account "the reasonable expectations of data subjects based on their relationship with the controller."
- Existence of a legitimate interest requires a "careful assessment" of whether there is "a relevant and appropriate relationship" and "whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place" (Recital 47).
- Highly fact- and context-specific analysis

Exemptions for research

GDPR: exemptions for research

- May avoid restrictions on secondary processing and on processing sensitive categories of data (Article 6(4); Recital 50)
- Override a data subject's right to object to processing and to seek the erasure of personal data (Article 89)
- Process personal data without the data subject's consent (Article 6(1)(f); Recitals 47, 157)
- Transfer personal data to third countries for research purposes (Article 49(h); Recital 113)

G. Maldoff, IAPP 2016; N. Bertels, 2016

Exemptions directly provided in the GDPR

- Article 17: right to have personal data erased when consent withdrawn or objection to processing, as well as when the data are no longer needed for the purpose for which they were first collected
- Complying with this right threatens the integrity of a researcher's dataset
- Regulation exempts research from the right to erasure insofar as it is "likely to render impossible or seriously impair the achievement of the [research] objectives" (Article 17(3)(d))
- At least in some cases, researchers may further process personal data for research purposes in spite of a data subject's request for erasure

Exemptions requiring member state legislative action

- Article 89(2) allows member states or the EU to limit data subject rights to access, rectification, restriction, and the right to object where processing is for research purposes subject to the appropriate safeguards
- Not a blanket authority to derogate from these rights
- Derogations must be "necessary for the fulfillment of [the research] purposes" and only permissible if allowing data subjects to exercise their rights likely would "render impossible or seriously impair the achievement of the specific purposes."

Exemption of notice for research

- Researcher may be exempt from the notice requirement if data received from someone other than the data subject
- Article 14 exempts controllers in these circumstances, if "the provision of such information proves impossible or would involve a disproportionate effort," which "could in particular be the case" in the research context (Recital 62)
- Researcher may claim exemption if providing notice would be "likely to render impossible or seriously impair the achievement of the [research] objectives," provided there are appropriate safeguards in place (Article 14(5)(b)).

Conditions for research exemptions (Article 89 protections)

- Controllers that process personal data for research purposes must implement "appropriate safeguards" (Article 89(1))
- "technical and organizational measures" to ensure that they process only the personal data necessary for the research purposes, in accordance with the principle of data minimization outlined in Article 5(c)
- Recital 33 states that controllers should act "in keeping with recognized ethical standards for scientific research."
- Those ethical standards are still being debated…

Secondary use of data not primarily collected for research

Secondary use

"while the GDPR explicitly permits re-purposing collected data for research, it also may permit a controller to collect personal data initially for research purposes, without requiring the data subject's consent"

(it may qualify under Article 6(1)(f) as a legitimate interest of the controller)

Secondary use for research

- Article 6(4) implies that a researcher may *further* process sensitive data for a research purpose, even if research was not the purpose for the initial collection
- Further processing is permissible when the subsequent processing is "compatible," such as for research (Recital 50).
- Even when special categories of personal data are processed, pursuant to Article 9" (Article 6(4))

GDPR's notice requirements

- Article 12(1) requires controllers to "take appropriate measures" to inform data subjects of the nature of the processing activities and the rights available to them
- Controllers are required to provide this information in all circumstances, regardless of whether consent is the basis for processing, "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12(1)).

Notice of processing data for research

- Notice should be provided at the time when the data is first collected and it must include the controller's identity and contact information, the intended purposes of the processing activities, and, where applicable, that the data will be transferred to another entity or to a third country.
- Additionally, a controller must provide, under Article 13(2), notice of the data subject's rights to access, rectification, erasure and to object to processing, as well as notice of "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period."

Difficulty in identifying research purposes in advance

- Providing up front notice about research at the point of collection poses a challenge for researchers
- Data mining techniques often search for correlations within data sets without the baseline of a specific test hypothesis
- Researcher may not know the scope of her research until after the data is collected and used
- Data subjects should be able to "consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

Secondary processing without consent

Myth associated with GDPR

"You must have consent if you want to process personal data."

While 'consent' is one of the six permitted ways to make processing lawful, it is not always the most appropriate.

And 'consent' may not be permitted as a justification for processing in a situation where there is an imbalance between the data subject and the controller making genuine freedom of choice impossible, such as an employment relationship.

Research without consent

"Research may furnish a legitimate basis for processing without a data subject's consent. The Regulation also allows researchers to process sensitive data and, in limited circumstances, to transfer personal data to third countries that do not provide an adequate level of protection."

"To benefit from these exemptions, researchers must implement appropriate safeguards, in keeping with recognized ethical standards, that lower the risks of research for the rights of individuals."

Source: Article 29 Working Party

Transfer of data

GDPR introduces a new basis for transferring data

- Under Article 49(1), a controller may transfer data to a third country when "necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject."
- Recital 113 makes clear that "the legitimate expectations of society for an increase of knowledge" should be taken into account when determining whether a "compelling legitimate interest" exists.

Transferring personal data to third countries for research purposes

- Prohibits the transfer of personal data to countries outside of the EU unless they offer an "adequate level of protection" as determined by the European Commission (Article 45(1))
- Controller may transfer personal data to a third country if it has implemented specific safeguards or if the data subject has provided explicit consent after being informed of the risks related to the transfer (Article 46(2); Article 49(1)(a))

National law required for scientific research

Article 9(2)(j) allows a researcher to process sensitive data where "processing is necessary for [research] purposes in accordance with Article 89(1) *based on Union or Member State law* which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

as clarified in Recital 52, research serves as a basis for processing sensitive data only "when provided by Union or Member State law and subject to suitable safeguards."

Conclusions

- GDPR preserves the equilibrium between data subjects' rights while allowing the processing of personal data, including sensitive data, for scientific research
- Cooperation duties and transparency between the actors of the processing, internally and with regard to the supervisory authorities
- Regulation provides new rights to data subjects, however, research remains widely regulated at national level
- Clear rules serve research practice regarding consent, reusing personal data for another purpose, assessing the risks of data processing, adopting accountable management system
- Respect of ethical standards as being part of the lawfulness of the processing in research