EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH


# The General Data Protection Regulation[1]: Secondary Use of Data for Medicines and Public Health Purposes

## Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

**Official address** Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
**Address for visits and deliveries** Refer to www.ema.europa.eu/how-to-find-us
**Send us a question** Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

# Table of Contents

## Executive Summary

Across the Member States of the Union there is a rich and diverse collection of health data and medical data, which are held in electronic form. This can include electronic health records (EHRs), laboratory information with diagnostic data, prescribing data, dispensing data, data from disease registries, health determinant data, datasets from (non-)interventional studies and of civil registrations including cause of death.

This important source of evidence holds huge potential to support public health and medicines development, regulation and decision-making across the Union. For the European Medicines Agency (EMA) this is of importance in supporting medicine development for the benefit of patients and enabling timely patient access to new medicines.

The potential for a strengthened evidence base for decision-making needs to respect applicable data protection rules, namely the General Data Protection Regulation (EU) 2016/679(GDPR) and Regulation (EU) 2018/1725 (EUDPR), which is applicable to EU institutions and bodies.

With these principles in mind and to deliver pharmaceutical innovation, research-performing/research-supporting infrastructures/platforms, data providers and medicines developers have identified the need for comprehensive guidance on the application of data protection rules, particularly on the secondary use of personal data for medicines and public health purposes. Processing of personal health data can have multiple purposes which are often categorised as "primary" and "secondary" (or further) purposes, the latter being defined as the use of health data (e.g., EHRs, health insurance claims data, registry data or drug consumption data) for other purposes than initially collected. This can refer to medicines development, safety monitoring, research and policy making..

To contribute to a better understanding of the GDPR and the secondary data use, EMA, in collaboration with the European Commission (EC) and other Union Agencies, has initiated the project "EHR: access, share, expand" under the Health Policy Agencies Collaboration (HPAC) programme. As part of the project, a set of "Questions and Answers (Q&As) on the GDPR and the Secondary Use of Data for Medicines and Public Health Purposes" will be developed with an aim to facilitating compliance with data protection rules and also helping patients and consumers in understanding their rights and the safeguards to protect personal data.

EMA understands that there are various stakeholders, which have different perspectives when it comes to the use of health data and medical data for the development, monitoring and evaluation of the quality, safety and efficacy of medicines.

Therefore, EMA is consulting in parallel interested stakeholders (grouped in two categories for the purpose of this consultation) by means of a dedicated discussion paper focusing on key topic areas, which are outlined below (chapters 3.1. to 3.9.). This follows an expression of interest to provide input to the drafting of the Q&As.

**EMA invites you to provide your data protection questions on secondary data use in the context of the GDPR focusing on 9 key topic areas.**

**Please send your contributions by 10 July 2020 to the following functional mailbox:**

dpconsultation@ema.europa.eu

# 1. Introduction

Across the Member States of the Union there is a rich and diverse collection of health data and medical data held in electronic form. This includes electronic health records (EHRs), laboratory information with diagnostic data, prescribing data, dispensing data, data disease registries data sets (e.g., cancer, immunisation), health determinant data, datasets from (non-)interventional studies and of civil registrations including cause of death.

In addition to patients, consumers and health care professionals, medicines developers, data providers and research-performing/research-supporting infrastructures are the contributors of this important source of evidence, which has a huge potential to support public health and medicines development, regulation and decision-making across the Union institutions, including Agencies, as well as Member States and other stakeholders.

Data collected in one country alone is often insufficiently powered to answer many of the public health questions that national authorities face, e.g. for rare disease exposed, rare outcomes or public health emergencies. Large data sets also provide a greater degree of precision and accuracy, and combining data across Member States provides information on national variations, on the effectiveness and impact of different public health interventions and strategies on larger numbers of patients, and may provide complementary types of information, which is important for regulatory and policy decision-making, both at Union and national levels. For EMA this is of particular importance as supporting medicine development for the benefit of patients and enabling timely patient access to new medicines is within its institutional remit.

The contribution of health data to clinical research, development and innovation would benefit regulatory science, notably with regard to exploring the identification of unmet need, allowing evidence collection where randomised clinical trials are impractical or unethical, and reducing cost of evidence generation or improved research quality.[2]

Processing personal health data can have multiple purposes. Often these purposes for processing health data are categorised as "primary" and "secondary" (or further) purposes. In this context, "primary" purposes are defined as those explicitly stated at the time of data collection, such as patient care, health system administration or research projects named at the time of data collection. "Secondary" (or further) purposes are those compatible with the primary purpose, that however were not explicitly stated at the time of data collection[3].[4] For example, when health data (e.g., electronic health records (EHRs), health insurance claims data, registry data or drug consumption data), which was collected in the course of primary care or research, is used by a health professional or medicines regulator for the purpose of performing their public tasks, this would be considered a secondary purpose – i.e. a secondary use of that data. Secondary use in the healthcare domain is also understood

[2] Cole, A. and Towse, A., 2018. Legal Barriers to Better the Better Use of Health Data to Deliver Pharmaceutical Innovation. OHE Consulting Report, London: Office of Health Economics. Available at: https://www.ohe.org/publications/legal-barriers-better-use-health-data-deliver-pharmaceutical-innovation

[3] See recital 50 and Article 5 of the GDPR

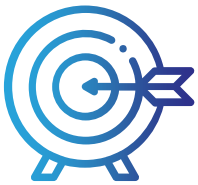
[4] Experts' Workshops Assessment of the Member States' rules on health data in the light of GDPR 2019/2020. Discussion Paper for Workshop 29 January, Brussels. Specific Contract No SC 2019 70 01 in the context of the Single Framework Contract Chafea/2018/Health/03, Executive Summary, page 5

as non-direct care use of personal health information, including but not limited to analysis, research, quality/safety measurement, public health and payment[5].

The potential for a strengthened evidence base for decision-making needs to respect applicable Union data protection legislation, namely the General Data Protection Regulation (EU) 2016/679 (GDPR), which is applicable to private and public entities in the Member States and Regulation (EU) 2018/1725 (EUDPR) which is applicable to EU institutions and bodies.

With these principles in mind and to deliver pharmaceutical innovation, many stakeholders have identified the need for comprehensive guidance on the application of data protection rules,[6],[7],[8],[9],[10] [11],[12] particularly on the secondary use of personal data for medicines and public health purposes.

## 2. Objectives



To contribute to a better understanding of the GDPR and the secondary data use, EMA, in collaboration with the European Commission (EC) and other Union Agencies, has initiated the project "EHR: access, share, expand" under the Health Policy Agencies Collaboration (HPAC) programme.

The objective of this project is to develop a set of "Questions and Answers (Q&As) on the GDPR and the Secondary Use of Data for Medicines and Public Health Purposes" with an aim to facilitating compliance with data protection rules and also helping patients and consumers in understanding their rights and the safeguards to protect personal data.
Although the Q&As will have no formal legal status, they will be intended to provide practical and technical guidance on how to comply with the GDPR. Also, it will address recommendations of the HMA-EMA Joint Big Data Taskforce to "ensure data are managed and analysed within a secure and ethical governance framework"[13].

[5] C. Safran et al. Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. J Am Med Inform Assoc. 2007 Jan-Feb; 14(1): 1–9. doi: 10.1197/jamia.M2273
[6] D. Peloquin et al. Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data. Eur J Hum Genet. 2020 Mar 2. doi: 10.1038/s41431-020-0596-x. [Epub ahead of print]
[7] S. Ayme. Enforcement of a new data protection law in Europe: A threat and an opportunity for registries and cohorts for rare diseases in the field of rare diseases. Article in La Revue de Médecine Interne 39(10) · April 2018. DOI: 10.1016/j.revmed.2018.03.013
[8] CA Behrendt et al. Clinical Registers in the Twenty-First Century: Balancing Act Between Data Protection and Feasibility? Chirurg 88 (11), 944-949. Nov 2017. PMID 29079875.
[9] MR Andersen et al. Cancer Registration, Public Health and the Reform of the European Data Protection Framework: Abandoning or Improving European Public Health Research? Eur J Cancer 51 (9), 1028-38. Jun 2015. PMID 24120502.
[10] DJ Kerr. Policy: EU Data Protection Regulation--Harming Cancer Research. Nat Rev Clin Oncol 11 (10), 563-4. Oct 2014. PMID 25178633.
[11] Federation of European Academies of Medicine. Use of data in cross-border biomedical research: what are the challenges ahead? Summary report of a workshop held on 20 November 2017. https://www.feam.eu/wp-content/uploads/FEAM-Forum_Data-workshop-report_Final.pdf
[12] Cole, A. and Towse, A., 2018. Legal Barriers to Better the Better Use of Health Data to Deliver Pharmaceutical Innovation. OHE Consulting Report, London: Office of Health Economics. Available at: https://www.ohe.org/publications/legal-barriers-better-use-health-data-deliver-pharmaceutical-innovation
[13] HMA-EMA Joint Big Data Taskforce Phase II report: 'Evolving Data-Driven Regulation'. https://www.ema.europa.eu/en/documents/other/hma-ema-joint-big-data-taskforce-phase-ii-report-evolving-data-driven-regulation_en.pdf

Furthermore, the Q&As are also intended as an input to the wider initiative of the EC to develop sector-specific legislative and non-legislative measures in the European Health Data Space (EHDS), which aims to foster the access to and sharing of different kinds of health data (e.g., electronic health records, genomics, registries) in Europe, whilst complying with the GDPR provisions.
The EC is currently working with Member States and stakeholders to define the necessary legal and governance framework, an interoperable infrastructure in support of the cross-border delivery of healthcare and to set up an appropriate infrastructure in support of the cross-border delivery of healthcare, as well as the use of quality health data and semantic interoperability for the development of new treatments, medicines, medical devices and services[14],[15].

## 3. Where and why do we seek your input?

EMA is consulting in parallel interested stakeholders. This follows an expression of interest to provide input in the drafting of the Q&As as set out in chapter 2.
For the purpose of the consultation, interested stakeholders are grouped in the following two categories:

- Patients and consumers as data contributors and
- Medicines developers, research performing and research-supporting infrastructures and other data providers (e.g., prescribing and dispensing data).

EMA understands that each of these stakeholder groups will have different perspectives when it comes to the use of health and medical data for the development, monitoring and evaluation of the quality, safety and efficacy of medicines.

EMA therefore invites you to share your experience and data protection questions on the secondary use of medical and health data focusing on 9 key topic areas which are reflected in figure 1 and which are further outlined in chapters 3.1. to 3.9.

**EMA would appreciate to receive your input and questions by 10 July 2020.**

**Please send your contributions to the following functional mailbox:**
**dpconsultation@ema.europa.eu**

[14] Experts' Workshops Assessment of the Member States' rules on health data in the light of the GDPR 2019/2020. Background Paper for Workshop on 16 March, Brussels, Specific Contract No SC 2019 70 01 in the context of the Single Framework Contract Chafea/2018/Health/03
[15] Joint Action addressing differences in national General Data Protection Regulation (GDPR) implementation in the health sector, including the European Health Data Space and the health data use.
https://ec.europa.eu/chafea/health/funding/joint-actions/documents/ja-european-health-data-space-2020_en.pdf

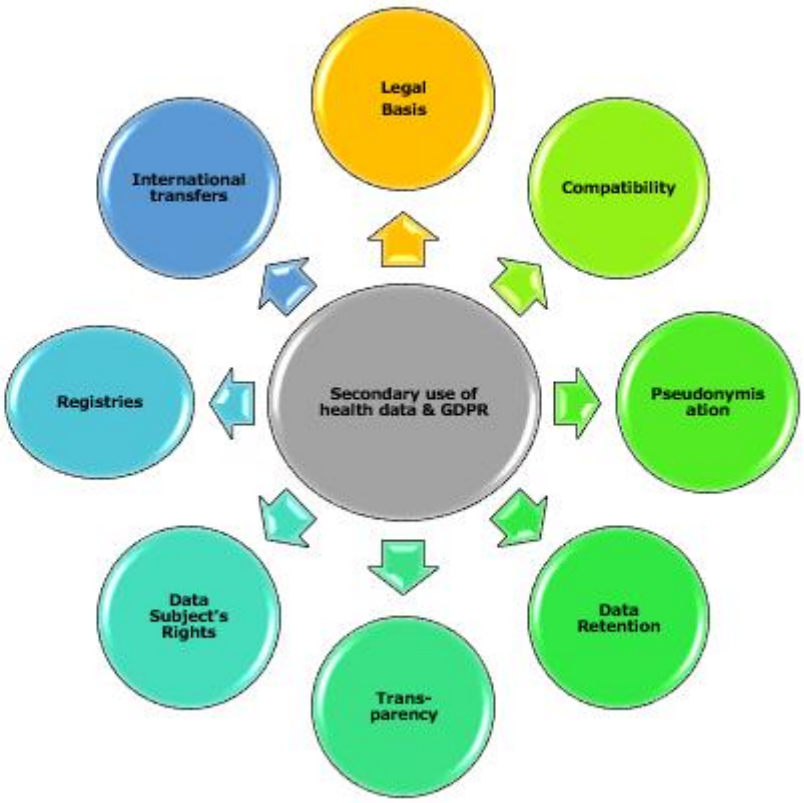



Figure 1: Nine data protection areas where EMA seeks your input on the secondary use of medical and health data in the context of the GDPR

## *3.1. Secondary use of health data*

The GDPR clarifies that personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject[16]. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services[17] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on e.g., a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test[18].

In a broader context, it may encompass self-reported data but also integration of emerging technologies such as personal sensing and geographic information systems (GIS)[19].

[16] See Recital 35 of the GDPR.
[17] as referred to in Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
[18] Ibid.
[19] J. A. Casey et al. Using Electronic Health Records for Population Health Research: A Review of Methods and Applications. Annual Review of Public Health Vol. 37:61-81 (Volume publication date March 2016). https://doi.org/10.1146/annurev-publhealth-032315-021353

Examples of secondary use of medical and health data are numerous:

- Drug utilisation studies such as use in different age groups (children) and off-label use;
- Relevance of clinical trial data versus clinical practice;
- Safety monitoring and evaluation;
- Planning and conduct of observational safety and effectiveness studies;
- (Comparative) effectiveness;
- Extrapolation of adult data to children or elderly;
- Conduct of pragmatic clinical trials;
- Identification of unmet medical needs;
- Monitoring the natural course of the disease following standard of care;
- Assessing disease incidence/prevalence;
- Establishing differences in clinical practice;
- Comparing of surrogate and clinical outcomes;
- Measuring background rates of events (for assessment of drug safety);
- Characterising the representativeness of patients in disease registries.

The framework for evidence generation during the life cycle of a medicine and the data types that support the evaluation of quality, safety and efficacy has been described by Cole and Towse (figure 2)[20]. Most of the refenced data types in figure 2 are processed based on the secondary (or further) use principle and can support the following medicines regulatory activities:

- the assessment of applications from sponsors for orphan designations to develop medicines designated to treat rare diseases (orphan medicines);
- the provision of scientific advice on the appropriate tests and studies to facilitate the development and availability of high-quality, effective and acceptably safe medicines, for the benefit of patients;
- the agreement on Paediatric Development Plans (PIPs) aimed at ensuring that the necessary data are obtained through studies in children to support the authorisation of a medicine for the paediatric population;
- the granting of marketing authorisations including conditional marketing authorisations of medicines aimed at treating, preventing or diagnosing seriously debilitating or life-threatening diseases and the fulfilment of requirements imposed on marketing authorisations granted under exceptional circumstances,
  and – from the side of applicants – the development of the dossiers and all relevant particulars and documents supporting a marketing authorisation application.

During the post-authorisation/supervision phase this can further refer to:

- individual case safety reporting, signal detection and management;
- submission and assessment of periodic safety update reports;

[20] Cole, A. and Towse, A., 2018. Legal Barriers to Better the Better Use of Health Data to Deliver Pharmaceutical Innovation. OHE Consulting Report, London: Office of Health Economics. Available at: https://www.ohe.org/publications/legal-barriers-better-use-health-data-deliver-pharmaceutical-innovation

- assessment of updates to risk management systems;
- post-authorisation studies sponsored or conducted by marketing authorisation holders (MAHs) on their own initiative or imposed on the MAH by law. This may include the conduct of a post-authorisation safety study if there are concerns about the risks of an authorised medicinal product or a post-authorisation efficacy study when the understanding of the disease or the clinical methodology indicate that previous efficacy evaluations might have to be revised significantly.

The GDPR states that processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected[21]. Furthermore, it is specified that:

- In such a case (i.e. processing for a compatible secondary purpose), no legal basis separate from that which allowed the collection of the personal data is required.
- If the 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.
- Further processing for scientific research purposes are considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing[22].

In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the following should be taken into account, inter alia:

- any link between those purposes and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;
- the nature of the personal data;
- the consequences of the intended further processing for data subjects;
- and the existence of appropriate safeguards in both the original and intended further processing operations[23].

EMA would be interested to learn from your experience and understand if there are questions on the secondary data use in the context of the GDPR and medicines and public health purposes.

[21] See Recital 50 of the GDPR.
[22] Ibid.
[23] Ibid.

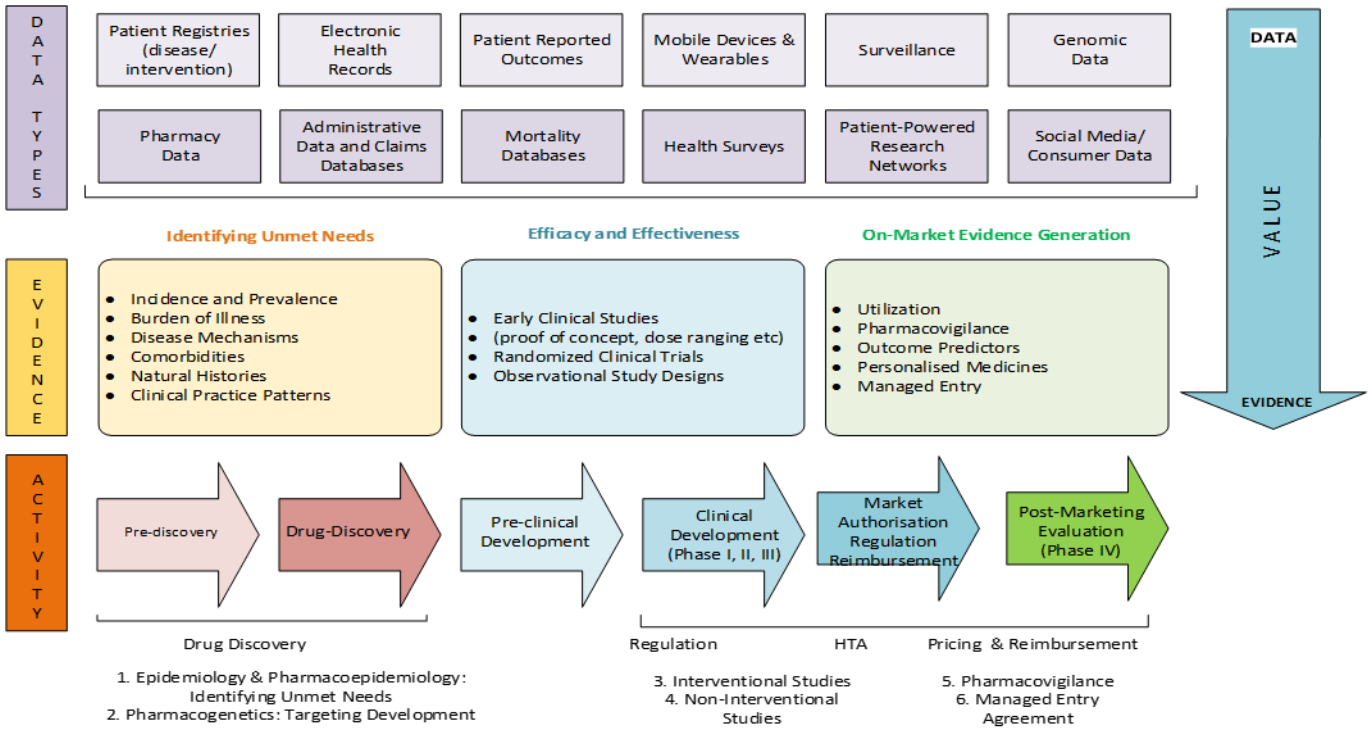



Figure 2: Based on "Framework for evidence requirements during the lifecycle of a medicines" [Cole, A. and Towse, A]

**Official address** Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
**Address for visits and deliveries** Refer to www.ema.europa.eu/how-to-find-us
**Send us a question** Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

### 3.2. Establishing the legal basis for processing personal data

According to the GDPR[24], processing shall be lawful only if and to the extent that at least one of the following applies:

- the **data subject has given consent to the processing of his or her personal data** for one or more specific purposes;
- 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;
- processing is necessary for **compliance with a legal obligation** to which the controller is subject;
- processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;
- 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;
- 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 which require protection of personal data, in particular where the data subject is a child. At any rate the existence of a legitimate interest needs careful assessment including 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. In this regard, the GDPR recognises that Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected[25].

Furthermore, the **processing of sensitive (health) data requires a specific justification**[26] such as:

- **Explicit consent** to the processing of those personal data for one or more specified purposes;
- To **protect the vital interests** of the data subject;

[24] See Article 6 of the GDPR.
[25] See Recital 49 of the GDPR.
[26] See Article 9(2) of the GDPR.

- Reasons of **public interest in the area of public health**, such as protecting against serous cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (on the basis of Union or national law).

Generally, the processing of special categories of personal data is prohibited, unless specific conditions are fulfilled[27]. As stated above, derogating from the prohibition on processing special categories of personal data is allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made amongst others for scientific research purposes[28]. It needs to be noted that Member States are allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data[29].

The EDPS has provided examples where EU Member States generally require prior consent from the participant in a research project for the processing of health data e.g.,

- Researchers, particularly in biobanking, increasingly rely on 'broad consent' to the use of data for further scientific research projects that are unknown at the time of collection, on the grounds that the risks are very low[30].
- For personal genome testing, 'tiered consent', where participants are invited to select from a set of options[31].
- 'Dynamic consent', where participants are asked to consent to different activities over time via an IT interface (trialled in the field of biobanks)[32].

The EDPS has pointed out that specific consent normally required under the GDPR may become less appropriate in the case of collected and inferred data and especially in the case of special categories of data on which much scientific research relies[33]. Recital 33 of the GDPR sets out that for scientific research purposes at the time of data collection it is often not possible to fully identify the purpose of personal data processing. Therefore, data subjects should be allowed to give consent to certain areas

[27] As listed in Article 9(2) of the GDPR.
[28] See Recital 52 of the GDPR
[29] See Recital 53 of the GDPR
[30] Mark Sheehan, 'Can broad consent be informed consent?' (November 2011), 4(3) Public Health Ethics 226; Graeme Laurie et al., 'A Review of evidence relating to harm resulting from uses of health and biomedical data' (30 June 2014), Nuffield Council on Bioethics. Referenced in "A Preliminary Opinion on data protection and scientific research". European Data Protection Supervisor, 6 January 2020, available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en
[31] Eline M. Bunnik et al., 'A tiered-layered-staged model for informed consent in personal genome testing' (21 November 2012), 21 European journal of human genetics 596. "Referenced in A Preliminary Opinion on data protection and scientific research. European Data Protection Supervisor, 6 January 2020, available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en"
[32] Kristin Solum Steinsbekk et al., 'Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem?' (September 2013), 21(9) European journal of human genetics 897. Referenced in "A Preliminary Opinion on data protection and scientific research. European Data Protection Supervisor, 6 January 2020, available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en"
[33] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, op. cit., p. 28. Referenced in "A Preliminary Opinion on data protection and scientific research. European Data Protection Supervisor 6 January 2020, available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and scientific_en

of scientific research when in keeping with recognised ethical standards for scientific research. Accordingly, data subjects should have an opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose[34]. The EDPS clarified in this regard that Recital 33 does not however take precedence over the conditions for consent set out in Articles 4(11), 6(1)(a), 7 and 9(2)(a) of the GDPR, and it requires the controller to carefully evaluate the rights of the data subject, the sensitivity of the data, the nature and purpose of the research and the relevant ethical standards[35]. Therefore, the EDPS continues, when research purposes cannot be fully specified, a controller would be expected to do more to ensure the essence of the data subject rights to valid consent are served, including through as much transparency as possible and other safeguards[36].

For the conduct of clinical trials under Regulation (EU) No 536/2014, the Clinical Trial Regulation (CTR), the EC[37] and the European Data Protection Board (EDPB)[38] have further clarified, that depending on all the circumstances of the trial and the concrete data processing activity, research related personal data processing may be carried out based on one of the following legal bases:

- The data subject's explicit consent [Article 6(1)(a) in conjunction with Article 9(2)(a) of the GDPR] or
- A task carried out in the public interest [Article 6(1)(e)] in conjunction with Article 9(2)(i) or (j) of the GDPR], or
- The legitimate interests of the controller [Article 6(1)(f) in conjunction with Article 9(2)(i) or (j) of the GDPR].

Furthermore, the EDPB[39] and the EC[40] both explained that informed consent[41] foreseen under the CTR must not be confused with the notion of consent as a legal ground for the processing of personal data under the GDPR. Consent under the GDPR must be freely given, specific, informed and unambiguous. Furthermore, where consent is used as a justification for processing special categories of data, such as health data, such consent must be explicit [Article 9(2) of the GDPR]. Depending on the circumstances of the clinical trial, situations of imbalance of power between the sponsor/investigator and participants may occur which may undermine the validity of (explicit) consent. Accordingly, data controllers should

[35] "A Preliminary Opinion on data protection and scientific research. European Data Protection Supervisor EDPS 6 January 2020, Section 6.3 on page 18 , available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en"
[36] See also the recent Guidance issued by the Association for German Supervisory Authorities on the interplay between recital 33 and the definition of consent in the GDPR (3 April 2019) confirms this approach. Referenced in "A Preliminary Opinion on data protection and scientific research. European Data Protection Supervisor, 6 January 2020, available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en"
[37] Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, European Commission Directorate-General for Health and Food Safety, available here: https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf
[38] European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), available here: https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en
[39] European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), available here: https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en
[40] Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, European Commission Directorate-General for Health and Food Safety, available here: https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf
[41] Article 28 of the CTR

conduct a particularly thorough assessment of the circumstances of the clinical trial before relying on individuals' consent as a legal basis for the processing of personal data for the purposes of the research activities of that trial.[42]

EMA would be interested to learn from your experience and understand if there are questions in establishing the legal basis for processing sensitive data in the context of the GDPR and secondary data use.

### 3.3. Presumption of compatibility

The GDPR states that processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected[43]. Furthermore, it is specified that:

- In such a case (i.e. processing for a compatible secondary purpose), no legal basis separate from that which allowed the collection of the personal data is required.
- If the 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.
- Further processing for scientific research purposes are considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing[44].

To ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected the following should be taken into account, inter alia:

- any link between those purposes and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;
- the nature of the personal data;
- the consequences of the intended further processing for data subjects;
- and the existence of appropriate safeguards in both the original and intended further processing operations[45].

The EDPS recently explained that the presumption of compatibility for research purposes depends on the requirement in Article 89(1) to ensure appropriate technical and organisational safeguards, such as pseudonymisation and access limitations[46] and that the data should not be used to support measures

[42] See European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), paragraphs 19 and 21, available here: https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en
[43] See Recital 50 of the GDPR.
[44] Ibid.
[45] Ibid.
[46] A Preliminary Opinion on data protection and scientific research. European Data Protection Supervisor, 6 January 2020, available here: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en

or decisions regarding any particular individuals[47]. Accordingly, the presumption of compatibility is not a general authorisation to further process data in all cases such as scientific purposes as stated by the EDPS and each case must be considered on its own merits and circumstances[48]. The EDPS concludes that in principle personal data collected in the commercial or healthcare context, for example, may be further used for scientific research purposes, by the original or a new controller, if appropriate safeguards are in place[49].

In this context the EDPB has stated that it intends to issue guidance on the "horizontal and complex" conditions for the applicability of the "presumption of compatibility" of further processing for archiving purposes in the public interest, scientific, historical research or statistical purposes, as provided for by the GDPR Article 5(1)(b)[50].

EMA would be interested to learn from your experience and understand if there are questions on the secondary use of data and the presumption of compatibility.

### *3.4. Pseudonymisation*

The principles of data protection apply to any information concerning an identified or identifiable natural person. Pseudonymisation means that personal data is processed in a manner that it can no longer be attributed to a specific data subject without the use of additional information (e.g. when a patient identification number is allocated to patients instead of using their other identifiers). This additional information (i.e. the code to identify the data subject) must be kept separately and securely.

Personal data which have undergone pseudonymisation is still considered information on an identifiable natural person[51], in other words it is still personal data. The GDPR further clarifies[52] that:

- In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.
- To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.
- The principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. The GDPR does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

[47] Ibid, with reference to Article 29 Working Party, Opinion 03/2013 on purpose limitation, op. cit., p.28
[48] Ibid.
[49] Ibid.
[50] European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), paragraph 31, available here: https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en.
[51] See Recital 26 of the GDPR
[52] Ibid.

We would be interested to learn from your experience and understand if there are questions on pseudonymisation in the context of the GDPR and secondary data use.

### 3.5. Data Retention

The GDPR sets out that personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.[53] It is further clarified[54] that:

- To ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.
- However, the further retention of the personal data should be lawful where it is necessary amongst others for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health for, scientific research purposes or statistical purposes.

EMA would be interested to learn from your experience and understand if there are questions on data retention in the context of the GDPR and secondary data use.

### 3.6. Transparency

The GDPR states that personal data should be processed lawfully, fairly and in a transparent matter[55]. It is further clarified[56] that:

- It should be transparent to the data subject as a natural person that his or her personal data are collected, used, consulted or otherwise processed. It should be clear to what extent the personal data are or will be processed.
- The principle of transparency requires that any information and communication relating to the processing of personal data is easily accessible and easy to understand, and that clear and plain language is used.
- A data subject is entitled to obtain information on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of your personal. The data subject also has the right to obtain confirmation and communication about what personal data concerning you are being processed.
- Data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.
- The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.

[53] See Recital 39 of the GDPR
[54] Ibid.
[55] Article 5(1((a) of the GDPR.
[56] See Recital 39 of the GDPR

EMA would be interested to learn from your experience and understand if there are questions on the transparency principles in the context of the GDPR and secondary data use.

### *3.7. Rights of the "data subject"*

Data subjects have the right of access to personal data which have been collected concerning themselves, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing[57]:

- This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.
- Every data subject therefore has the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.
- Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.
- That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.
- Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.
- The GDPR provides for a data subject to have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes the GDPR or Union law to which the controller is subject[58].
- A data subject has the right to have personal data concerning him or her erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of personal data does not otherwise comply with the GDPR.
- Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.[59]
- The GDPR provides mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The

[57] See Recital 63 of the GDPR
[58] See Recital 65 of the GDPR
[59] See Recital 39 of the GDPR

controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

- The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.[60]

EMA would be interested to learn from your experience and understand if there are questions on the rights of data subjects in the context of the GDPR and secondary data use.

### 3.8. Registries

The GDPR acknowledges that by coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression[61]. On the basis of registries, research results can be enhanced, as they draw on a larger population. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services.

In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law[62].

EMA would be interested to learn from your experience and understand if there are questions on secondary data use from registries.

### 3.9. International Transfers

When personal data is transferred outside the European Economic Area (EEA), special safeguards are foreseen to ensure that the protection travels with the data. The GDPR offers a diversified toolkit of mechanisms to transfer data to third countries such as[63]:

- **Adequacy decisions**: The EC has the power to determine, by the adoption of an adequacy decision on the basis of Article 45 of the GDPR whether a country outside the EU offers an adequate level of data protection.[64] It is important to clarify that three of the adequacy decisions[65] adopted by the EC so far apply to the transfer of data to commercial organisations only (as opposed to public institutions or international organisations established in these countries).

[60] See Recital 64 of the GDPR
[61] See recital 157 of the GDPR
[62] Ibid.
[63] Rules on international data transfers, European Commission website:https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/rules-international-transfers-personal-data_en
[64]Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[65] The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan (commercial organisations), Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with South Korea.

Where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards[66].

Such appropriate safeguards are listed in Article 46 of the GDPR as follows:

- **Standard data protection clauses**: The EC may adopt standard contractual clauses (SCC) to be used as standard data protection clauses to ensure sufficient safeguards for the data to be transferred internationally between the parties of the SCC[67]. So far it has issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or EEA and one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA[68]. Standard data protection clauses may also be adopted by data protection supervisory authorities of Union Member States provided that they are also approved by the EC.
- **Binding corporate rules**: Group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data[69].
- **Certification mechanism and codes of conduct**.
- **Legally binding and enforceable instrument** between public authorities or bodies or provisions to be inserted into administrative arrangements between such bodies which include enforceable and effective data subject rights. Latter provisions are subject to the authorisation of the competent data protection supervisory authority of the Member State concerned.
- **Contractual clauses** may be also agreed between the data exporter and data importer to provide appropriate safeguards for the transfers. Such "ad-hoc" contractual clauses are always subject to the authorisation of the competent data protection supervisory authority of the Member State concerned.

Personal data may be also subject to international transfer in the case of specific situations listed in Article 49 of GDPR (so-called "derogations")[70].
In accordance with Recital 111 of the GDPR allows the possibility of transfers in certain circumstances:

- where the data subject has given his or her **explicit consent**,

[66] See Recital 114 of the GDPR
[67] Standard Contractual Clauses (SCC). Standard contractual clauses for data transfers between EU and non-EU countries. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
[68] Ibid.
[69] See Recital 111 of the GDPR
[70]See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, available here: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en

- where the **transfer is occasional and necessary in relation to a contract or a legal claim**, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies,
- where **important grounds of public interest laid down by Union or Member State law so require**,
- where the **transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest**. In this case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register. This also applies when the register is intended for consultation by persons having a legitimate interest, where the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

These derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities or for public health, for example in the case of contact tracing for contagious diseases[71].

Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable [72].

For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer[73].

EMA would be interested to learn from your experience and understand if there are questions on international transfers in the context of the GDPR and the secondary data use e.g., in multi-national studies.

[71] See Recital 112 of the GDPR
[72] See Recital 113 of the GDPR
[73] Ibid.

## 4. Next Steps

Your input will be used for determining the content of the "Q&As on the GDPR and the Secondary Use of Data for Medicines and Public Health Purposes" (see chapter 2).

EMA will consolidate your input and will aim to put your questions in context of operational scenarios such as medicine development, marketing authorisation approvals and post-authorisation safety monitoring.

At the end of the drafting phase of the Q&As, EMA will launch a targeted consultation to receive your feedback. This is anticipated for Q4 2020. This will be followed by a consultation of the EC and the EDPS with a publication anticipated in of the 1st half of 2021.

## 5. Glossary of terms and definitions

| Term | Reference | Description |
|---|---|---|
| public Health | Regulation (EC) No 1338/2008[74] | All elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. |
| electronic health record (EHR) | C. Safran et al.<br>Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper.<br>J Am Med Inform Assoc. 2007 Jan-Feb; 14(1): 1–9. doi: 10.1197/jamia.M2273 | Personal data created, developed, maintained, and/or provided by clinicians, providers, and allied health providers in direct patient care; an electronic application containing health information about individuals that is used by clinicians, providers, and allied health professionals to provide direct care for the individuals. |
| data concerning health | Article 4(15) of the GDPR | means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. |
| genetic data | Article 4(13) of the GDPR | means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. |
| Biometric data | Article 4(14) of the GDPR | means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the |

[74] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16December 2008 on Community statistics on public health and health and safety at work. Official Journal L. 2008;354:70

| Term | Reference | Description |
|---|---|---|
| | | unique identification of that natural person, such as facial images or dactyloscopic data. |
| personal data | Article4(1) of the GDPR | means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| processing | Article 4(2) of the GDPR | means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| pseudonymisation | Article 4(5) of the GDPR | means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; |
| controller | Article 4(7) of the GDPR | means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria |

| Term | Reference | Description |
|---|---|---|
| | | for its nomination may be provided for by Union or Member State law. |
| consent | Article 4(11) of the GDPR | of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. |
| primary use of data | C. Safran et al.<br><br>Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper.<br><br>J Am Med Inform Assoc. 2007 Jan-Feb; 14(1): 1–9. doi: 10.1197/jamia.M2273 | the use of personal health information by the organisation or entity that produced or acquired these data in the process of providing real-time, direct care of an individual. |
| secondary use of data | C. Safran et al.<br><br>Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper.<br><br>J Am Med Inform Assoc. 2007 Jan-Feb; 14(1): 1–9. doi: 10.1197/jamia.M2273 | non-direct care use of personal health information including but not limited to analysis, research, quality/safety measurement, public health (with modification). |