

WHITE PAPER

TRANSPARENT PROCESSING OF HEALTHCARE AND SOCIAL WELFARE DATA: INFORMATION WITH ICONS

Marjut Salokannel
Eveliina Ignatius
Teppo Vesikukka

Translation Mikko Keinänen

Data literacy for
responsible
decision-making



Data
Lit



TRANSPARENT PROCESSING OF HEALTHCARE AND SOCIAL WELFARE DATA: INFORMATION WITH ICONS



WHITE
PAPER
3/2023

SUMMARY

Transparent processing of personal data is a basic principle of the regulation of data protection in the EU. We cannot influence the processing of personal data if we don't know that they are processed in the first place. **The data controller has a legal obligation** to provide information concerning the processing of personal data. This obligation fulfils the transparency principle

3 FACTS ABOUT THE DATA PROTECTION REGULATION

- ① The provided information must be clear, easily accessible, and easy to understand. The controller also has the obligation to facilitate the exercise of data subjects' legal rights.
- ② In the healthcare and social welfare sector, wellbeing services counties are the main data controllers. Transparency requirements, including the inherently linked obligation to inform, are the responsibility of the wellbeing services counties.
- ③ The EU General Data Protection Regulation allows for the visualization of information through standardised icons. Combining written information with icons symbolising different purposes of processing personal data also enables better consideration of the needs of specific groups and enhances the accessibility of the information.

RECOMMENDATION

In support of provided information, we recommend the use of icons for the visualization of the processing of healthcare and social welfare data and for the support of information obligations of the controller. Here we present a set of draft icons and explain the content of the obligation to inform data subjects. The icons can be used to visualize both the responsibilities of the data controller and the rights of the data subject. They can also make the information more accessible to the data subjects.

Icons can be downloaded from
www.datalit.fi/tietosuojakuvakkeet



WRITERS:

Marjut Salokannel, marjut.salokannel@helsinki.fi
Eveliina Ignatius, eveliina.ignatius@helsinki.fi

ICONS, GRAPHIC DESIGN, LAYOUT:

Teppo Vesikukka, teppo.vesikukka@aalto.fi

TRANSLATION:

Mikko Keinänen

DataLit is an interdisciplinary collaboration between social science, law, and computer science that develops understandable and trustworthy practices for utilizing Finnish health, social, and welfare data. The collaborating partners include many national public data authorities and organisations.

The research project is funded by the Strategic Research Council which is associated with the Academy of Finland.

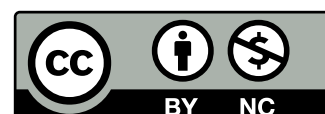
www.datalit.fi

Twitter: @DataLit_SRC

ISBN 978-951-51-9025-3

Creative Commons License
Attribution-NonCommercial 4.0 International

<https://creativecommons.org/licenses/by-nc/4.0/legalcode.fi>



Contents

TRANSPARENT PROCESSING OF HEALTHCARE AND SOCIAL WELFARE DATA: INFORMATION WITH ICONS	I-II
1. CHANGING EUROPEAN REGULATORY FRAMEWORK FOR PROCESSING HEALTHCARE AND SOCIAL WELFARE DATA	1
1.1. Protection of personal data is a fundamental right	
1.2 Legislative framework	1
1.3 Information obligation of the controller	3
2 TRANSPARENCY REQUIREMENTS FOR PROCESSING PERSONAL DATA	4
2.1 General principles concerning transparent processing of personal data	5
2.2 Children and other vulnerable persons	6
2.3 Information to be provided to the data subject where personal data are collected directly from the data subject (GDPR Article 13)	7
2.3.1. General	7
2.4 Further information facilitating the exercise of rights (GDPR 13.2)	8
3. INFORMING ABOUT SECONDARY USE	11
3.1. Informing about secondary use when data are collected directly from the data subject	11
3.2 Information about secondary use by Findata, THL and other potential controllers concerning secondary use of healthcare and social welfare data	13
4. OPTIONS FOR THE PRACTICAL IMPLEMENTATION OF INFORMATION	16
5. INFORMATION WITH VISUAL ICONS	16
Sources	22

1. CHANGING EUROPEAN REGULATORY FRAMEWORK FOR PROCESSING HEALTHCARE AND SOCIAL WELFARE DATA

1.1. PROTECTION OF PERSONAL DATA IS A FUNDAMENTAL RIGHT

Article 8 of the Charter of Fundamental Rights of the European Union (EU) provides that everyone has the right to the protection of personal data. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Therefore, the EU General Data Protection Regulation (GDPR)¹ makes it mandatory for the controller to inform about the purposes and the legal basis of processing of personal data when the personal data are collected directly from the data subject and in principle also when they are collected from other sources. The character of data protection as a fundamental right entails that any limitation thereof has to fulfil the requirements of article 52.1 of the Charter of Fundamental Rights, and it is not possible to limit the essential content of the right.

The Constitution of Finland (731/1999) protects personal data as part of the right to privacy provided for in section 10 of the Constitution. In the healthcare and social welfare sector, the confidentiality of patient and client data (hereinafter **healthcare and social welfare data**) constitutes an essential part of the protection of the privacy of patients and clients of social services. As healthcare and social welfare data is particularly sensitive, clients and patients must be able to trust that the data remains confidential throughout its lifecycle. At national level, the confidentiality of healthcare and social welfare data is guaranteed in the Act on the Openness of Government Activities (621/1999) and in legislation relating to the status of clients of social services (Act on the Status and Rights of Social Welfare Clients 812/2000) and rights of patients (Act on the Status and Rights of Patients 785/1992). In addition, national legislation provides a relatively detailed regulation for the use of healthcare and social welfare data.

1.2 LEGISLATIVE FRAMEWORK

Healthcare and social welfare data are processed **for a primary purpose** within primary and specialised healthcare as well as in social welfare, for example when treatment or care is provided. The collected data can also be

¹ Regulation (EU) 2016/679 of the European parliament and of the Council 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)

used in a so-called **secondary purpose**, that is for statistics, scientific research and innovation, education and training, planning and knowledge-based management.

The regulatory basis for the processing of healthcare and social welfare data is the EU General Data Protection Regulation (GDPR). It is further specified in national legislation, which is currently undergoing change due to new provisions on processing of health data proposed within the health and social services reform. Moreover, the regulatory framework will undergo changes with the new regulations of the EU.

At the national level, the regulation relating to the processing of healthcare and social welfare data is changing through the comprehensive reform of information management in healthcare and social welfare. The new law aims at a clearer and more coherent regulation of information management, including data processing, in healthcare and social welfare.² The law also takes into account the transparency principle, in particular as to informing the patients and clients of social services on the primary use of their data.

The regulatory environment is changing also at EU level. On 3 May 2022, the EU Commission submitted its proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (EHDS).³ The proposal can be seen to reproduce at EU level the context in which health data are used in Finland. In Finland, secondary use is regulated by the Act on Secondary Use of Healthcare and Social Welfare Data (552/2019), hereinafter Secondary Use Act, that entered into force in 2020. In the proposed Regulation, primary use concerns granting cross-border access to a patient's main care related health data, the so called patient data summary, when the patient is receiving healthcare in another member state. Secondary use covers all purposes in the Finnish Secondary Use Act, but it also contains certain new purposes, such as the use of health data for training of AI applications and use of data for personalised medicine. When adopted, the proposal would constitute binding legislation taking precedence over national law, which means it would be appropriate to take it into account of when informing data subjects about possible further uses of their data.

As the context in which healthcare and social welfare data are processed is both widening and becoming more complex, it is important that the basic principles of data processing and the rights and obligations of the various

² HE 246/2022 vp

³ COM/2022/197 final

actors are clarified to all users of the data and to all residents in Finland. The aim of this policy paper is to promote the **transparent processing of data**. To enhance transparency and increase the efficiency of informing about processing of personal data, we focus in this policy paper on clarifying and operationalising the obligations of controllers to **inform** data subjects of different primary and secondary uses of their data, as required in the GDPR and further implementing it to Finnish national laws and practices.

1.3 OBLIGATION OF THE CONTROLLER TO INFORM DATA SUBJECTS

Who is the data controller in the new processing environment of healthcare and social welfare data?

According to the GDPR, **data controller** 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” (GDPR 4.1(7)). The data subject refers to a natural person whose personal data is collected, processed and stored by the controller. Within healthcare and social welfare, the **data subject** is a client or a patient. Even healthcare staff have the status of data subject in the information systems of service providers.

In Finland, according to the Act on Organising Healthcare and Social Welfare Services (612/2021), hereinafter the Organising Act, **the wellbeing services county** acts as the controller of healthcare and social welfare client and patient data that are created in the activities which it is responsible for organising, or that have been transferred to it from municipalities and joint municipal authorities. **Therefore, the obligation to provide information to data subjects and facilitating the use of their rights, is the responsibility of the wellbeing services county.**

The controller of national level information systems is regulated in the Act on Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021), which provides that the Social Insurance Institution of Finland acts as the controller of the MyKanta data repository, the log data storage service of the disclosure log registry, and the operation logs related to its own activities.

It should be noted that the definition of controller depends on the GDPR and the national specifying sectoral legislation. The role of controller is not a contractual matter. Hence, the wellbeing services county acts as the

controller also when services are purchased from private service providers, for example as an outsourced service.⁴ Then the private service provider, when offering an outsourced public service, is a processor of personal data within the meaning of the GDPR. Considering this, the responsibilities and obligations of the controller in accordance with the GDPR remain with the wellbeing services county.

According to the GDPR, the processor of personal data is the actor which processes personal data on behalf of the controller. Where a processor makes independent decisions about the processing of personal data, it becomes a joint controller together with the original controller regarding the processing of those personal data about which it exercises independent decision-making power. This also applies to private service providers if they provide own services along with public services. The private service provider is the controller of the personal data included in the services of its own, private service provision.

2. TRANSPARENCY REQUIREMENTS FOR PROCESSING PERSONAL DATA

Processing personal data in a transparent way is a fundamental principle of European data protection law. Personal data shall be processed lawfully, fairly and *in a manner which is transparent to the data subject*.⁵

Transparent processing has been deemed to include three central areas:

- ① The provision of information related to fair processing of data to data subjects;
- ② The way in which controllers inform data subjects about their rights under the GDPR; and
- ③ The ways in which controllers facilitate the exercise by data subjects of their rights.⁶

In order for us to know which of our personal data have been collected, how they are used and how we can have access to them, the law requires that the data subjects must be informed of the collecting of personal data and their further processing purposes.⁷ **This is an obligation of the data controller. The main principle of processing of personal data is that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.** The transparency requirement of

⁴ Organising Act, section 58; see also HE 241/2020 vp, p. 797

⁵ GDPR 5.1a

⁶ EU Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, WP260, as last revised and adopted on 11 April 2018, p. 4

⁷ See GDPR Articles 12-14

processing is applicable throughout the lifecycle of the personal data.⁸ **At any time, the controller must be able to demonstrate that it has informed the data subjects of the processing of their personal data in accordance with GDPR.**

Data subjects must be informed of the processing of their data before the data is collected. The information must cover all the uses of the personal data that are known at the time, including further processing of the data for different purposes on the basis of the Finnish Secondary Use Act or legal requirements by law and the right of the data subject to object to this further processing.⁹

2.1 GENERAL PRINCIPLES RELATING TO TRANSPARENT PROCESSING OF PERSONAL DATA

According to the GDPR, the processing of personal data shall be transparent and shall clearly indicate from which source the personal data are collected, how they are used and what rights the data subject has regarding the use of their personal data.¹⁰ The controller shall provide detailed information to the data subject about the processing of personal data and their rights pursuant to the GDPR. The information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The GDPR authorises the use of icons in electronic form to help clarify the information.¹¹ According to the regulation, the information may be provided to data subjects in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. The icons should be machine-readable. The GDPR specifically mentions standardised icons, but so far no action has been taken within the EU to create and implement such standardised icons. Even research on icons and on how to create and standardise them has been relatively rare.

The information on the processing of healthcare and social welfare data could be visualised and clarified, in accordance with the GDPR, through electronic icons and accompanying text. This would make it possible for the controller to adapt the information to clients' and patients' varying needs and levels of understanding.

⁸ WP260, p. 6

⁹ CJEU C-268/21 Norra Stockholm Bygg AB, ECLI:EU:C:2023:145

¹⁰ Ks. TSA 12 artikla

¹¹ TSA 12.7 Artikla

Here we would also like to raise the possibility of linking the icons to the MyKanta data repository, which constitutes the national E-health record repository including health and social services data from both public and private service providers.

2.2 CHILDREN AND OTHER VULNERABLE PERSONS

Special attention should be paid that the information is clear and intelligible, in particular when the personal data of children and other vulnerable persons are processed. According to WP29, transparent processing of personal data is a free-standing right, which means that information about the processing should be provided also to a child throughout the lifecycle of the processing irrespective of the fact that consent may have been given originally by the holder of parental responsibility over the child. Information given to a child should be formulated in a way that the child can easily understand it.¹²

Specific protection of children in the context of the requirement of transparent processing of personal data is highlighted in the GDPR. In addition to children, the WP29 considers that the controller should take account of the vulnerability of even other groups, including people with disabilities. At the same time, the controller should assess the data subjects' likely level of understanding.¹³ In practical terms, taking account of different groups of people in information means, for example, accessibility to information. The content and form of Information should therefore take account of persons who may have difficulties in understanding plain language text or a digital processing environment. Likewise, the rights of persons with limited vision or illiterate persons have to be taken into account, for example by adding audible material from a recording to the information.

The UN Convention on the Rights of Persons with Disabilities¹⁴ – to which the EU is also a party – sets requirements for accessibility that apply also to information, communications and electronic services. The Convention also requires the States Parties to ensure that private entities that offer services which are open to the public take into account aspects that are relevant for accessibility. Correspondingly, the Convention guarantees access to information on an equal basis with others (Article 21) and requires States Parties to protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others

¹² WP260, s.10

¹³ WP260, s.11

¹⁴ See <https://social.desa.un.org/issues/disability/crpd/convention-on-the-rights-of-persons-with-disabilities-crpd>

(Article 22). Receiving information in an accessible way is a crucial precondition for the realization of other rights.

The information should also consider linguistic rights. The information material should be provided in Finnish and Swedish and, to the extent possible, in another language widely used in a wellbeing services county. In the Sámi region, information has to take account of the provisions of the Sámi Language Act (1086/2003). Here it should be noted that even a private service provider must follow the Sámi Language Act when it fulfils tasks outsourced to it according to the law by a public service provider.

2.3 INFORMATION TO BE PROVIDED TO THE DATA SUBJECT WHERE PERSONAL DATA ARE COLLECTED DIRECTLY FROM THE DATA SUBJECT (GDPR ARTICLE 13)

2.3.1 GENERAL

Article 13 of the GDPR provides for the minimum information that the controller shall, before starting to process personal data, always provide to the data subject, i.e. to the person from whom the data is collected. This refers to cases in which the data subject has knowingly provided their personal data to the controller. The data controller is considered **to collect personal data directly from a data subject also when this happens by observation, for example using automated data capturing devices or data capturing software**. WP29 guidelines mention as examples cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors.¹⁵

In the healthcare and social welfare sector, the information obligation of the data controller includes at least the following information:

- ① The contact details of the controller and, where applicable, the joint controllers, and, for each data controller, the contact details of the data protection officer.
- ② **The purposes** of the processing for which the personal data are intended as well as **the legal basis** for the processing;
 - Here it should be noted that in principle there can be only one legal basis for the processing of personal data for each purpose. This is essential with regard to the exercise by the data subject of his or her rights.
 - If the processing of personal data is based on legitimate interests (GDPR 6.1 (f)), the controller must indicate its own or a third

¹⁵ WP260, p. 15

party's legitimate interests. Here it should be emphasised that legitimate interests cannot be invoked to justify processing carried out by public authorities in the performance of their tasks

- ③ Recipients or categories of recipients of the personal data;
Are the data possibly transferred to countries outside the European Economic Area, and if so, is the country in question included among countries approved by the EU Commission as offering an adequate level of data protection. If this is not the case, what is the legal basis of the possible transfer pursuant to GDPR. In this connection it should be recalled that even the use of cloud computing services of third countries within the EU has to comply with the requirements of the GDPR regarding transfer of personal data to third countries.

2.3.2. FURTHER INFORMATION FACILITATING THE EXERCISE OF RIGHTS (GDPR 13.2)

In the GDPR, transparent processing of personal data also means **the controller's obligation to facilitate the exercise of data subjects' rights**. For the data subjects to be able to exercise their rights, they should be provided the following information, in addition to the minimum information about the processing:

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- Information on the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as information on the right to data portability;
- Where the processing is based on consent pursuant to GDPR (point (a) of Article 6(1) or point (a) of Article 9(2)), information on the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent **before** its withdrawal. In this context it should be borne in mind that in the public sector, processing of personal data should in principle not be based on consent. There are situations, however, in which consent is requested, and in such cases the data subject has to be explained if it is a consent to the processing of personal data or, for example, consent as a safeguard to the processing.

- Information on the right to lodge a complaint with a supervisory authority;
 - Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
 - Information on the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Information obligations shall be taken into account of also when personal data are processed for a secondary use, i.e. for a purpose other than the primary use. **The data subject shall be informed of all the different secondary use purposes and the data subject's possibilities to exercise their rights regarding them.** This has been stated in the recent cases of the Court of Justice "Norra Bahnhof" and "Österreichische Post". ¹⁶

¹⁶ CJEU Case C-154/21 "Österreichische Post", ECLI:EU:C:2023:3

Primary use of healthcare and social welfare data

The Secondary Use Act defines primary use as the purpose for which personal data were first stored. In the healthcare sector, this means providing healthcare to a patient, and information is given by the municipal health centre or the hospital district. In the private sector, information is given by the private service provider acting as the data controller.

Secondary use

According to the Secondary Use Act, use for secondary purposes means processing of personal data for purposes other than in primary use. For example, data collected for the purpose of providing healthcare to a patient (primary purpose) can be used for a secondary purpose in scientific research. Secondary purposes provided for in the Secondary Use Act are scientific research, statistics, development and innovation, steering and control activities by public authorities, planning and analysis by public authorities, education and training, and knowledge-based management. If the controller intends to further process personal data for purposes other than the one for which the data were first collected, the controller shall inform the data subject about this other purpose before the further processing and provide all relevant additional information about this processing, unless they have already been provided when the personal data were collected. This specifically includes processing of healthcare and social welfare data for a secondary purpose. In Finland, secondary uses are regulated in the Secondary Use Act. Even if the law doesn't contain provisions with regard informing data subjects the relevant provisions of the GDPR must be complied with. This means that tools to inform data subjects could be included in healthcare and social welfare data information processing systems.

The provisions of article 13 of GDPR are mandatory, which means that there can be no derogations from them. It is not sufficient information to say that personal data are processed according to the law. The only possible derogation is in case the controller can show that the data subject already has the information in question.

¹⁵ CJEU Case C-154/21 "Österreichische Post", ECLI:EU:C:2023:3

3. INFORMING ABOUT SECONDARY USE

3.1 INFORMING ABOUT SECONDARY USES WHEN DATA ARE COLLECTED DIRECTLY FROM THE DATA SUBJECT

The information about possible secondary uses must also take place when the controller collects the personal data from the data subject for the first time. This concerns those purposes of which the controller is aware at the moment of collecting the data. It includes all purposes based on law, because the controller is obliged to know the content of the laws. In case the controller later uses the personal data for another purpose, the data subjects must be informed about that purpose. In the healthcare and social welfare sector, this concerns above all the wellbeing services counties but

SPECIAL CASE: Automated decision-making

According to Article 22 of the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her or similarly significantly affects him or her. Automated decision-making is permitted, however, in the cases mentioned in Article 22.2, for example when the decision is authorised by national law to which the controller is subject and which also lays down suitable measures to safeguard rights and freedoms and legitimate interests.

Within social welfare, automated decision-making can mean an administrative decision and/or profiling based on predictive analytics that can have significant effects on an individual, in which case it is subject to Article 22 of the GDPR and requires informing the data subject, i.e. the person subject to the automated decision-making.

Automated decision-making within the meaning of Article 22 of the GDPR can also occur within healthcare, where it does not necessarily refer to an administrative decision, but rather to other decisions regarding for example the health status of a data subject or the accessibility of healthcare services.¹⁷

However, data subjects must always be informed about automated decision-making, regardless of whether it has significant effects for an individual within the meaning of Article 22 of the GDPR. In that situation, the information must in any case include the elements mentioned in Article 14 of the GDPR, above all the legal basis of the processing, the controllers, from which source the personal data originate, how data subjects can exercise their rights, and how automated decision-making possibly affects them.

¹⁷ Decisions 3895/83/2022 and 6482/186/2020 of the Deputy Data Protection Ombudsman

also organisations collecting data for secondary uses such as THL and Findata.

Uses within the meaning of the Secondary Use Act are:

- ① Statistics
- ② Scientific research
- ③ Development and innovation
- ④ Education and training
- ⑤ Knowledge-based management; including predictive analytics
- ⑥ Steering and control activities by public authorities within healthcare and social welfare
- ⑦ Planning and analysis by public authorities

In this context, the information should cover at least:

- notification about the different uses and about how the data subject can exercise their rights regarding each use. The information should clearly indicate
- which entity the data subject can contact to exercise their rights if the exercise of rights is not possible within the Kanta services. Currently, data subjects cannot exercise their rights regarding secondary use through the MyKanta data management system.

In Denmark, the data protection authority has given a notice to the healthcare district of the Region of Southern Denmark about not informing the patients clearly enough that residual biological material from diagnostic samples will be transferred to the regional biobank and that the patient has the right to prohibit the use of the sample for any other purpose than their immediate treatment. **The data protection authority explicitly states that reference to general privacy policy statements accessible through a hyperlink is not enough, even if the information in question is included there. In addition, it has to be ensured that patients who are especially vulnerable are informed in an intelligible manner about the use of samples and their personal data and about their right regarding that use.**¹⁸

¹⁸ Datatilsynet, Case No. 2021-432-0059.

3.2 INFORMATION OBLIGATION OF FINDATA AND THL RELATING TO SECONDARY OF USE OF HEALTHCARE AND SOCIAL WELFARE DATA

Data subjects must be informed about secondary use by the controllers responsible for the secondary processing of personal data in the same way as when the personal data has been collected directly from the data subject. Information must also be provided about the source from which the personal data has been collected (GDPR 14.2(f)). Information should be provided within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed. If a disclosure to another recipient is envisaged, as in the case of Findata for example, information should be provided at the latest when the personal data are first disclosed (GDPR 14.3).

Findata and the Finnish Institute for Health and Welfare (THL) have both decided that, as a rule, they will not inform data subjects individually regarding their activities, but will invoke the possibility of an exception provided in GDPR 14.5(b), according to which information is not required, if the provision of the information:

- ① proves impossible; or
- ② would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) of GDPR, or
- ③ in so far as informing the data subject of the processing is likely to render impossible or seriously impair the achievement of the objectives of that processing;

In such cases the GDPR provides that the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Findata issues data permits for scientific research and statistical purposes. It can also issue permits based on data requests relating to processing of data for innovation purposes, in which case the data is provided in table or aggregated format. Findata publishes on its website the names of the

projects for which it has issued permits. There are short descriptions of the research projects in the Findata website.

According to the Secondary Use Act, controllers may authorise Findata to issue permits on their behalf, including in cases where only their data is used for a secondary purposes. THL has given such an authorisation to Findata regarding projects other than the ones in which it is not involved itself. Further information about the permits Findata has issued can be found on its website.¹⁹

THL publishes on its website information about research projects that it has financed and/or that have used its data. Biobanks also publish on their own websites information about research using their data or about other collaboration agreements, such as with pharmaceutical industry. However, hospital districts' websites usually do not include information about individual research projects, notwithstanding certain exceptions.

In the information practices relating to the use of data according to the Secondary Use Act account of should be taken of the recent European Data Protection Board opinion on the proposal for a Regulation on the European Health Data Space. According to the opinion, the possibility provided for in the GDPR to exempt, in certain cases, the data controller from informing each individual data subject, when the personal data has been collected from a source other than the person themselves, cannot be applied systematically to secondary uses of health data. The permit authority acting as the controller should analyse whether data subjects should be informed individually about the use of their personal data in a particular project, or whether the requirements in GDPR Article 14.5 regarding an exemption from individual information are fulfilled for that project. The EDPB highlights that the EHDS proposal should be considered in the light of Article 23 of the GDPR, which includes provisions for a Member State to derogate from certain rights of data subject guaranteed in the GDPR.²⁰

¹⁹ <https://findata.fi/en/permits/>

²⁰ European Data Protection Board and the European Data Protection Supervisor: EDPB-EDPS Joint Opinion 2022/03, paragraph 96.

SPECIAL CASE: Medical research

Medical research can be a primary purpose for processing health data, when the data are collected directly from the research subject. The Act on Medical Research (488/1999, as amended by 984/2019), hereinafter the Research Act, sets as a starting point the patient's informed consent to participate in a medical research. In practice this means that in medical research, the collection of patient data is based on consent, but this consent is not the basis of the processing of personal data, but rather **the legal basis of this processing is derived directly from the Research Act**. According to the Research Act, **the legal basis of processing is Article 9.2(i) of GDPR, if the processing is necessary for reasons of public interest in the area of public health. This requires that the research subject has given their informed consent to participate in the research.**

However, the Act does not prohibit processing of personal data based on consent given in accordance with the GDPR. Here it should be recalled that each specific purpose of processing of personal data presupposes one legal basis for processing pursuant to the GDPR. The controller cannot list more than one legal bases for processing just to be sure, as it were, but rather the information should indicate the legal basis of processing for each processing operation.

The controller has to inform the data subject of the processing of personal data according to the GDPR. Therefore, in addition to informing about the primary and secondary uses, **the information should also indicate what effect the withdrawal of the consent regarding participation in the research has on the processing of personal data.**

Clinical trials within the meaning of the EU Regulation on Clinical Trials (Regulation (EU) No 536/2014) are subject to the Regulation itself, but also to the Act on Clinical Trials (983/2021) and partly to the Research Act.

ERITYISTAPAUUS: Quality registers

In the autumn of 2022, the Act on the Finnish Institute for Health and Welfare (668/2008), hereinafter the THL Act, was amended to include the maintenance of national quality registers as one of the tasks of the THL, (section 2 point 4(d)). A quality register, within the meaning of the law, is a register of data to be used to assess the treatment of a specific illness, or a method of treatment, or a social service. The register is used to store necessary personal data related to an illness and a method of treatment or to the provision of social welfare. In addition, it can be used to store data about the operational unit responsible for the treatment or service and the persons who carried it out, in order to assess the quality of the treatment or service.

In other words, the register can include identifiable personal data of both healthcare staff and of patients and clients. Pursuant to the Secondary Use Act, these data can be processed for purposes that are in accordance with the Secondary Use Act. The THL can combine personal data collected for different purposes and registers in order to carry out its statutory tasks. An exception to this are the personal data that the THL collects as a statistical authority for statistical purposes, because the processing of such data is possible only pursuant to the Act on Statistics (280/2004). Other actors can have access through Findata, and according to the Secondary Use Act, to the quality registers for which THL is responsible as controller.²²

Currently there are nine quality registers for which the Ministry of Social Affairs and Health has ordered the THL to be responsible as controller. These are the diabetes register, HIV register, renal disease register, psychosis treatment quality register, register for back-related diseases, quality register for the treatment of mouth and tooth related diseases, heart register, critical care quality register, and quality register for inflammatory rheumatic diseases.²²

^{21, 22} Decree STM 2022/116 of the Ministry of Social Affairs and Health on Quality Registers of the Finnish Institute for Health and Welfare, and the memorandum thereto

4. OPTIONS FOR THE PRACTICAL IMPLEMENTATION OF INFORMATION OBLIGATIONS

- ① Information issued by hospital districts, occupational healthcare and private service providers (websites and printed material), with a link to the MyKanta section of Kanta services.
 - Clear distinction between primary use and secondary use
 - Link regarding secondary use to the information management section of the relevant data controller (for example THL, Findata) if the exercise of rights is resolved at this level

- ② Information management service located at the MyKanta within the Kanta services

- ③ Information on individual secondary uses is given by the relevant data controllers

EHDS includes provisions on project-specific information on data controllers' websites and on how an individual data subject can exercise their rights regarding the project.

- ④ Future integration of uses pursuant to EHDS into the information management system











Possible with the same icons added with new uses:

- Secondary processing of health data in training of AI applications
- Processing of health data for the treatment of other patients, that is personalised medicine

5. INFORMATION WITH VISUAL ICONS

The GDPR provides for a preference for as clear and accessible information as possible on the processing purposes of personal data. The Regulation specifically mentions information with the help of visual machine-readable icons. Clicking on the icon the data subject can get more information on the purpose in question.

Categories

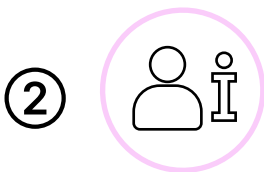
-  I. Obligation of the controller to inform about the processing of personal data
-  II. Right to request and access the data
-  III. Right to rectify the data
-  IV. Right to erase the data
-  V. Right to restrict the processing of data
-  VI. Right to object to processing of data
-  VII. Right to data portability
-  VIII. Right to know about automated decision-making, including profiling
-  IX. Right to complain to a supervisory authority
-  * Does not apply in the healthcare and social welfare sector

Icons



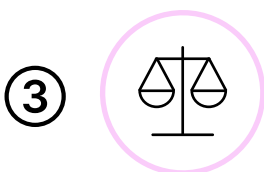
Data controller and contact details

The controller processing personal data shall provide information about the controller, eventual representative of the controller, and their contact details.



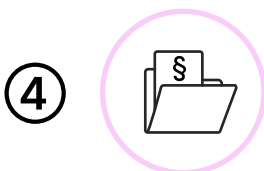
Data protection officer and contact details

The controller shall provide information about the data protection officer and their contact details.



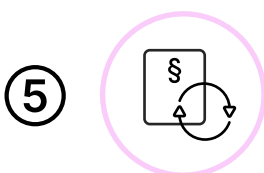
Legal basis of processing

The controller shall declare the legal basis of the processing of personal data in accordance with the GDPR. The legal basis of the processing of healthcare and social welfare data can be for example a statutory task, public interest and relevant specifying legislation, or consent.



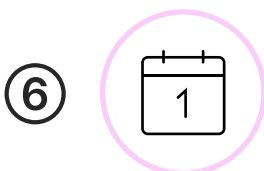
Primary purpose of processing

The primary purpose of processing is the purpose for which the data are collected. For example, patient data collected for the provision of treatment or care.



Secondary purpose of processing

The secondary purpose of processing is any other purpose of processing than the primary purpose. For example, data collected for the purpose of providing healthcare to a patient can be used for a secondary purpose in scientific research.



Period for which personal data are stored

The controller shall declare the period for which the personal data will be stored or the information necessary to determine that period. This will ensure that the processing is fair and transparent. To minimise the processing of personal data, that period shall be as short as possible. There is separate legislation on the periods of storage of client and patient data.

7



Which data are collected?

The controller's obligation to inform applies to all personal data collected, including for example data collected later from other sources and data to be combined with the original data.

8



Who has access to the data?

The right of access to client and patient data of healthcare and social welfare professionals is based on their professional tasks. A professional has the right to access and to use the data that are necessary to fulfil their tasks (Act on Client Data, section 15).

The data subject has a statutory right to request access to all the log data concerning their personal data.

According to the Act on Client Data, the client shall be provided on their written request the information about who has used the data concerning them, to whom they have been disclosed and what has been the purpose of the use and disclosure. The information shall be provided free of charge, but the service enabler may charge a reasonable fee for information requested a second time concerning the same time period.

A service enabler in the healthcare and social welfare sector is obliged by the Act on Client Data to maintain a register of the users of its own data registers and the access rights of those users.

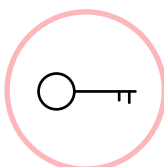
9



Processor of personal data

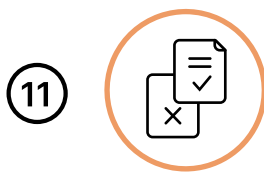
The processor of personal data processes personal data on behalf of the controller. The processing shall take place only on instructions from the controller. The responsibilities of the controller remain with the controller. In the healthcare and social welfare sector, the processor of personal data can be for example a private service provider from which the wellbeing services county purchases services that it is responsible for organising..

10



Access to own personal data

The data subject has the right to obtain, free of charge, access to their own data (Article 15 GDPR). The data subject has the right to obtain confirmation as to whether or not their personal data concerning are being processed, and the right of access to that data. A confirmation shall be given also if the data are not processed. The personal data may not be erased before providing access to them.



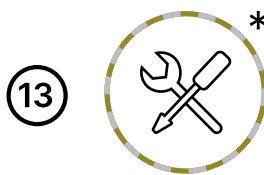
Rectification of data

The data subject has the right to request the rectification of their own personal data. In the healthcare and social welfare sector, this right is in practice affected by the national legislation regulating client and patient data.



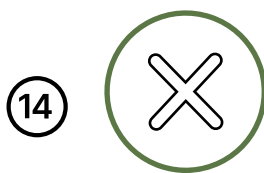
Erasure of data *

The data subject has the right to request the erasure of their own personal data. This right does not mean that the controller always has the obligation to erase the data. For example, the legislation concerning patient data within healthcare includes an obligation for healthcare professionals to draw up patient records and to keep them.



Right to restrict the processing of data *

The data subject has the right to request the restriction of the processing of their own personal data. Especially within the public healthcare and social welfare sector, this right is affected by the national legislation regulating client and patient data.



Right to object to processing of data

The data subject has the right to object, on grounds relating to their particular situation, to the processing of their personal data, when the processing is based on public interest. In the private sector, the basis of processing can also be a legitimate interest, in addition to public interest. A controller who, notwithstanding the objection, wishes to process the data, shall demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

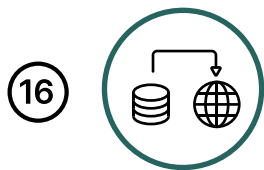
Where personal data are processed for scientific research purposes or statistical purposes applying the safeguards pursuant to the GDPR, the controller can, notwithstanding the objection by the data subject on grounds relating to their particular situation, process the personal data, if the processing is necessary for the performance of a task carried out for reasons of public interest.

This right is not the same as the so-called 'opt-out', which makes it possible, in cases provided by law, to prohibit the processing of personal data.



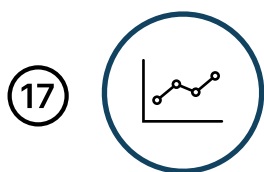
Right to data portability

The data subject has the right in principle to transmit the personal data concerning them to another controller if the processing is based on consent and is carried out by automated means. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.



Transfer of personal data to third countries

The data subject has the right to know if the personal data are processed in countries outside the European Economic Area or by a service provider, such as a cloud computing service, established in such a country. They have the right to know whether the level of data protection in that country is equivalent to that ensured within the EU.

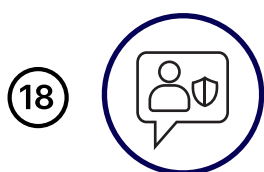


Right to know about automated decision-making

The data subject has the right to know about automated decision-making. Decision-making based solely on automated processing, which produces legal effects concerning the data subject or similarly significantly affects them, is permitted only in situations provided for in Article 22.2 of GDPR.

Automated decision-making based on health data or on other personal data of special categories of data is possible, according to GDPR, only on the basis of explicit consent or legislation safeguarding the data subject's rights.

In Finland, the automated decision-making by public authorities will be based in the future for the most part on the proposed general law (HE 145/2022 vp). The general law would not apply to health data nor constitutionally sensitive data, such as social welfare data.



Right to complain to a supervisory authority

The data subject has the right to complain to a supervisory authority. In Finland, the competent supervisory authority is the Data Protection Ombudsman.

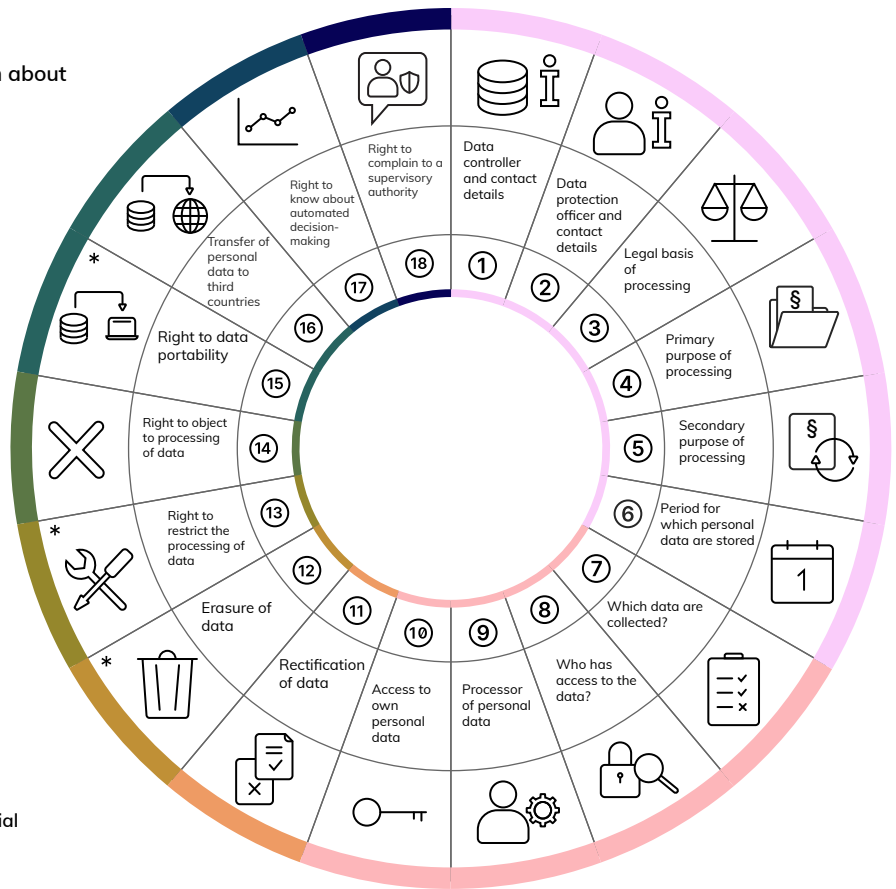
Infographic and summary of icons:

Information on the processing of data: Data Lit

Obligation of the controller and the rights of the data subjects

Rights of the data subject

- I. Obligation of the controller to inform about the processing of personal data
- II. Right to request and access the data
- III. Right to rectify the data
- IV. Right to erase the data
- V. Right to restrict the processing of data
- VI. Right to object to processing of data
- VII. Right to data portability
- VIII. Right to know about automated decision-making, including profiling
- IX. Right to complain to a supervisory authority
- * Does not apply in the healthcare and social welfare sector



Data protection icons

① Data controller and contact details

The controller shall provide information about the controller, eventual representative of the controller, and their contact details.



② Data protection officer and contact details

The controller shall provide information about the data protection officer and their contact details.



③ Legal basis of processing

The controller shall declare the legal basis of the processing of personal data in accordance with the GDPR. The legal basis of the processing of healthcare and social welfare data can be for example a statutory task, public interest and relevant specifying legislation, or consent.



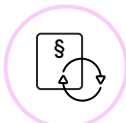
④ Primary purpose of processing

The primary purpose of processing is the purpose for which the data are collected. For example, patient data collected for the provision of treatment or care.



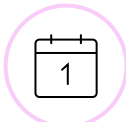
⑤ Secondary purpose of processing

The secondary purpose of processing is any other purpose of processing than the primary purpose. For example, data collected for the purpose of providing healthcare to a patient can be used for a secondary purpose in scientific research.



⑥ Period for which personal data are stored

The controller shall declare the period for which the personal data will be stored or the information necessary to determine that period. To minimise the processing of personal data, that period shall be as short as possible.



⑦ Which data are collected?

The controller's obligation to inform applies to all personal data collected, including for example data collected later from other sources and data to be combined with the original data.



⑧ Who has access to the data?

The data subject has a statutory right to request access to all the log data concerning their personal data.



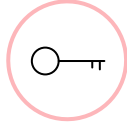
⑨ Processor of personal data

The processor of personal data processes personal data on behalf of the controller. The processing shall take place only on instructions from the controller. The responsibilities of the controller remain with the controller.



⑩ Access to own personal data

The data subject has the right to obtain, free of charge, access to their own data (Article 15). The data subject has the right to obtain confirmation as to whether or not their personal data concerning are being processed, and the right of access to that data.



⑪ Rectification of data

The data subject has the right to request the rectification of their own personal data.



⑫ Erasure of data

The data subject has the right to request the erasure of their own personal data. This right does not mean that the controller always has the obligation to erase the data.



⑬ Right to restrict the processing of data

The data subject has the right to request the restriction of the processing of their own personal data.



⑭ Right to object to processing of data

The data subject has the right to object, on grounds relating to their particular situation, to the processing of their personal data, when the processing is based on public interest or legitimate interests. The controller can, however, process the personal data, if it can demonstrate compelling legitimate grounds for the processing which override the rights of the data subject.



⑮ Right to data portability

The right to data portability provided for in Article 20 of the GDPR is normally not applied in the healthcare and social welfare sector, because the processing is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.



⑯ Transfer of personal data to third countries

The data subject has the right to know if the personal data are processed in countries outside the European Economic Area or by a service provider, such as a cloud computing service, established in such a country. They have the right to know whether the level of data protection in that country is equivalent to that ensured within the EU.



⑰ Right to know about automated decision-making

The data subject has the right to know about automated decision-making, such as profiling. The controller has the obligation to ensure the protection of the data subject's rights and freedoms and legitimate interests in accordance with the GDPR.













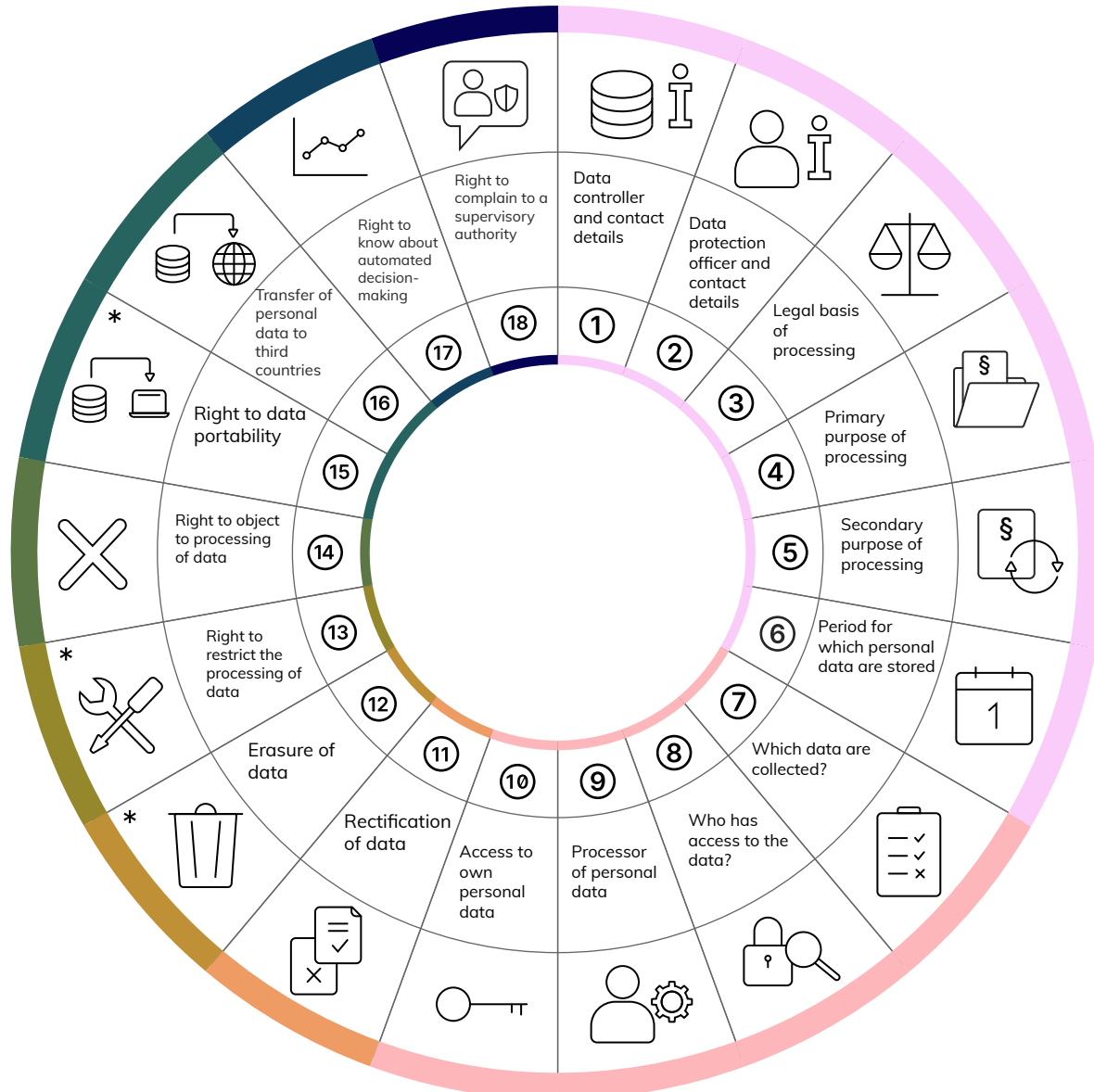
⑱ Right to complain to a supervisory authority

The data subject has the right to complain to a supervisory authority. In Finland, the competent supervisory authority is the Data Protection Ombudsman.



Data privacy notice and rights

-  I. Obligation of the controller to inform about the processing of personal data
-  II. Right to request and access the data
-  III. Right to rectify the data
-  IV. Right to erase the data
-  V. Right to restrict the processing of data
-  VI. Right to object to processing of data
-  VII. Right to data portability
-  VIII. Right to know about automated decision-making, including profiling
-  IX. Right to complain to a supervisory authority
-  * Does not apply in the healthcare and social welfare sector



Data protection icons

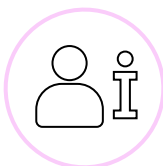
① Data controller and contact details

The controller shall provide information about the controller, eventual representative of the controller, and their contact details.



② Data protection officer and contact details

The controller shall provide information about the data protection officer and their contact details.



③ Legal basis of processing

The controller shall declare the legal basis of the processing of personal data in accordance with the GDPR. The legal basis of the processing of healthcare and social welfare data can be for example a statutory task, public interest and relevant specifying legislation, or consent.



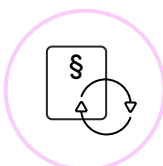
④ Primary purpose of processing

The primary purpose of processing is the purpose for which the data are collected. For example, patient data collected for the provision of treatment or care.



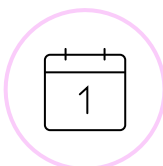
⑤ Secondary purpose of processing

The secondary purpose of processing is any other purpose of processing than the primary purpose. For example, data collected for the purpose of providing healthcare to a patient can be used for a secondary purpose in scientific research.



⑥ Period for which personal data are stored

The controller shall declare the period for which the personal data will be stored or the information necessary to determine that period. To minimise the processing of personal data, that period shall be as short as possible.



⑦ Which data are collected?

The controller's obligation to inform applies to all personal data collected, including for example data collected later from other sources and data to be combined with the original data.



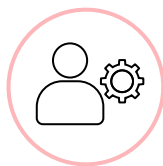
⑧ Who has access to the data?

The data subject has a statutory right to request access to all the log data concerning their personal data.



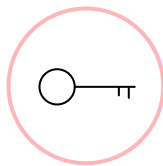
⑨ Processor of personal data

The processor of personal data processes personal data on behalf of the controller. The processing shall take place only on instructions from the controller. The responsibilities of the controller remain with the controller.



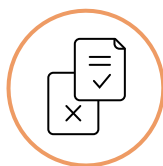
⑩ Access to own personal data

The data subject has the right to obtain, free of charge, access to their own data (Article 15). The data subject has the right to obtain confirmation as to whether or not their personal data concerning are being processed, and the right of access to that data.



⑪ Rectification of data

The data subject has the right to request the rectification of their own personal data.



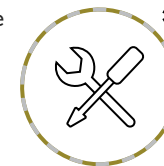
⑫ Erasure of data

The data subject has the right to request the erasure of their own personal data. This right does not mean that the controller always has the obligation to erase the data.



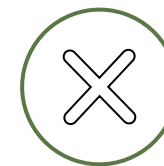
⑬ Right to restrict the processing of data

The data subject has the right to request the restriction of the processing of their own personal data.



⑭ Right to object to processing of data

The data subject has the right to object, on grounds relating to their particular situation, to the processing of their personal data, when the processing is based on public interest or legitimate interests. The controller can, however, process the personal data, if it can demonstrate compelling legitimate grounds for the processing which override the rights of the data subject.



⑮ Right to data portability

The right to data portability provided for in Article 20 of the GDPR is normally not applied in the healthcare and social welfare sector, because the processing is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.



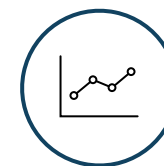
⑯ Transfer of personal data to third countries

The data subject has the right to know if the personal data are processed in countries outside the European Economic Area or by a service provider, such as a cloud computing service, established in such a country. They have the right to know whether the level of data protection in that country is equivalent to that ensured within the EU.



⑰ Right to know about automated decision-making

The data subject has the right to know about automated decision-making, such as profiling. The controller has the obligation to ensure the protection of the data subject's rights and freedoms and legitimate interests in accordance with the GDPR.



⑱ Right to complain to a supervisory authority

The data subject has the right to complain to a supervisory authority. In Finland, the competent supervisory authority is the Data Protection Ombudsman.



SOURCES

EUROPEAN UNION:

- Charter of Fundamental Rights of the European Union
- General Data Protection Regulation of the EU (Regulation (EU) 2016/679 of the European parliament and of the Council 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)
- European Union Regulation on clinical trials (Regulation (EU) 536/2014 of the European parliament and of the Council, of 16 April 2014, on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (Text with EEA relevance))
- Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)197/2)

EU CASE LAW:

- Case C-268/21 Norra Stockholm Bygg AB, EU:C:2023:145
- Case C-154/21 Österreichische Post, EU:C:2023:3

NATIONAL LEGISLATION:

- Act on Clinical Trials (983/2021)
- The Act on Medical Research (488/1999)
- Act on Patient Rights and Status (785/1992)
- Act on Social Welfare Client Documents (254/2015)
- Act on Social Welfare Client Rights and Status (812/2000)
- Act on Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021)
- Act on Organising Healthcare and Social Welfare Services (612/2021)
- Act on Secondary Use of Healthcare and Social Welfare Data (552/2019)
- Act on the Finnish Institute for Health and Welfare (668/2008)
- Act on the Openness of Government Activities (621/1999)
- Sámi Language Act (1086/2003)
- The Constitution of Finland (731/1999)

- Data Protection Act (1050/2018)
- Act on Statistics (280/2004)

NATIONAL DECREES:

- Decree of the Ministry of Social Affairs and Health on Patient Documents (STM 94/2022)
- Decree of the Ministry of Social Affairs and Health on Quality Registers of the Finnish Institute for Health and Welfare (STM 2022/116)
- Government Decree on Medical Research (989/1999)

OFFICIAL SOURCES OF THE EUROPEAN UNION:

- EU Data Protection Working Party Guidelines on transparency under Regulation 2016/679, WP260, as last revised and adopted on 11 April 2018
- European Data Protection Board and the European Data Protection Supervisor: EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space. Available at: https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en_.pdf

INTERNATIONAL OFFICIAL SOURCES:

- Datatilsynet, Case No. 2021-432-0059, available at: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/okt/datatilsynet-udtaler-kritik-af-region-hovedstaden>

NATIONAL OFFICIAL SOURCES:

- Decision 3895/83/2022 of the Deputy Data Protection Ombudsman
- Decision 6482/186/2020 of the Deputy Data Protection Ombudsman
- HE 145/2022 vp
- HE 241/2020 vp
- HE 246/2022 vp
- Decree of the Ministry of Social Affairs and Health STM/2022/116, explanatory memorandum.