World Health Organization
REGIONAL OFFICE FOR Europe

The protection of personal data in health information systems – principles and processes for public health

World Health Organization
REGIONAL OFFICE FOR Europe

The protection of personal data in health information systems – principles and processes for public health

Abstract

In recent years, countries across Europe have implemented either new or considerably stricter data protection and cybersecurity laws. These laws continue to have a substantive impact on health information systems (HISs) and most public health activities in a wider sense. This document aims to explore the conceptual implications and to give some guidance on how specific decisions that are unavoidable to balance the rights and interests at stake should be taken.

With a few easy-to-implement steps, any organization in public health can increase its level of data protection compliance significantly. As data protection is based on principles that have evolved over time, section 2 gives a short historical overview, followed by a deep dive into the legal principles behind data protection. Section 3 covers the practical implications of these principles and addresses the rights of data subjects, as these are at the heart of the regulatory framework. Section 4 examines the elements that need to be balanced against these rights – in particular, the right to health and to public health in general. Section 5 looks again at the secondary use of data for public health purposes, and at how the balancing of the interests at stake works in this context. Finally, section 6 gives an overview of the steps to be taken to make this happen, such as empowerment and oversight mechanisms.

This guidance document is part of the WHO Regional Office for Europe's work on supporting Member States in strengthening their health information systems. Helping countries to produce solid health intelligence and institutionalized mechanisms for evidence-informed policy-making has traditionally been an important focus of WHO's work and continues to be so under the European Programme of Work 2020–2025.

Keywords:
HEALTH INFORMATION SYSTEMS, DATA PROTECTION, DATA SECURITY, COMPUTER SECURITY

WHO/EURO:2021-1994-41749-57154

© World Health Organization 2021

Some rights reserved. This work is available under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO licence (CC BY-NC-SA 3.0 IGO; https://creativecommons.org/licenses/by-nc-sa/3.0/igo).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited, as indicated below. In any use of this work, there should be no suggestion that WHO endorses any specific organization, products or services. The use of the WHO logo is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the World Health Organization (WHO). WHO is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition: The protection of personal data in health information systems – principles and processes for public health. Copenhagen: WHO Regional Office for Europe; 2021".

Any mediation relating to disputes arising under the licence shall be conducted in accordance with the mediation rules of the World Intellectual Property Organization. (http://www.wipo.int/amc/en/mediation/rules/)

Suggested citation. The protection of personal data in health information systems – principles and processes for public health. Copenhagen: WHO Regional Office for Europe; 2020. Licence: CC BY-NC-SA 3.0 IGO.

Cataloguing-in-Publication (CIP) data. CIP data are available at http://apps.who.int/iris.

Sales, rights and licensing. To purchase WHO publications, see http://apps.who.int/bookorders. To submit requests for commercial use and queries on rights and licensing, see http://www.who.int/about/licensing.

Third-party materials. If you wish to reuse material from this work that is attributed to a third party, such as tables, figures or images, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the copyright holder. The risk of claims resulting from infringement of any third-party-owned component in the work rests solely with the user.

General disclaimers. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of WHO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted and dashed lines on maps represent approximate border lines for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by WHO in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by WHO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall WHO be liable for damages arising from its use.

Contents

Acknowledgements

This document was developed by the Data, Metrics and Analytics Unit in the Division of Country Health Policies and Systems of the WHO Regional Office for Europe. The main author is Tobias Schulte in den Baeumen. Marieke Verschuuren and David Novillo Ortiz provided direction during the production of the report and technical advice during concept drafting, writing and review. Special thanks to Natasha Azzopardi-Muscat for her strategic guidance.

For further information please contact the Data, Metrics and Analytics Unit (euhiudata@who.int).

Aim of this guidance

This guidance document is part of WHO Regional Office for Europe's work on supporting Member States in strengthening their health information systems (HISs). Helping countries to produce solid health intelligence and institutionalized mechanisms for evidence-informed policy-making has traditionally been an important focus of WHO's work and continues to be so under the European Programme of Work 2020–2025.[1]

One of the instruments WHO uses in this work is HIS assessments. A common finding in these assessments across Member States in the WHO European Region is problems in the production of health statistics as a result of data protection frameworks that are not appropriately geared to enable use of secondary data for statistical and research purposes. WHO has therefore developed this guidance as part of its HIS strengthening toolkit.

1 European Programme of Work. In: WHO/Europe [website]. Copenhagen: WHO Regional Office for Europe; 2020 (https://www.euro.who.int/en/health-topics/health-policy/european-programme-of-work/european-programme-of-work). All URLs accessed 3 November 2020.

Abbreviations

DPIA	data protection impact assessment
EU	European Union
GDPR	General Data Protection Regulation
HIS	health information system
ISO	International Organization for Standardization
IT	information technology

1. Introduction and scope

In recent years, countries across Europe have implemented either new or considerably stricter data protection and cybersecurity laws. These laws continue to have a substantive impact on health information systems (HISs) and most public health activities in a wider sense. While data protection – or rather, the fundamental right behind the concept of data protection – receives widespread recognition, it should be noted that this right is not absolute but needs to be balanced with other fundamental rights and public interests, such as the right to health. This document aims to explore the conceptual implications and to give some guidance on how specific decisions that are unavoidable to balance the rights and interests at stake should be taken.

While the ambition is to provide hands-on advice, it seems crucial to explore the concepts and principles of data protection first. Notably, data protection is not rocket science, as it requires clearly defined steps that can be followed in both design and implementation of a health information management system. Equally, data protection compliance is not particularly costly, in terms of either human resources or technology investments. With a few easy-to-implement steps, any organization in public health can increase its level of data protection compliance significantly. This guidance aims to give some insight into the "doing" of data protection.

As data protection is based on principles that have evolved over time, section 2 gives a short historical overview, followed by a deep dive into the legal principles behind data protection. Section 3 covers the practical implications of these principles and addresses the rights of data subjects, as these are at the heart of the regulatory framework. Section 4 examines the elements that need to be balanced against these rights – in particular, the right to health and to public health in general. While public health is in a privileged position overall, it is clearly bound by the same standards as any other domain in terms of information technology (IT) security. Section 5 looks again at the secondary use of data for public health purposes, and at how the balancing of the interests at stake works in this context. Finally, section 6 gives an overview of the steps to be taken to make this happen, such as empowerment and oversight mechanisms.

2. History of data protection and its fundamental principles

2.1 History and definitions

In 1890, two American lawyers, Samuel D. Warren and Louis Brandeis, wrote "The right to privacy", an article that argues that individuals have a "right to be left alone", using the phrase as a definition of privacy.[2] In 1948, the Universal Declaration of Human Rights was adopted, including the twelfth fundamental right: the right to privacy.[3] As technological advances accelerated, so the legal frameworks of data protection evolved. In 1980, the Organisation for Economic Co-operation and Development issued guidelines on data protection in direct response to the increasing use and power of computers to process data.[4] A year later, the Council of Europe adopted the Data Protection Convention – Convention 108 – which was the first time the right to privacy was enshrined into law for European countries.[5] Initially, the regulatory framework was supposed to protect the individual citizen from intrusions into their privacy by the state.

In late 1983, the Federal Constitutional Court of Germany reached a fundamental decision regarding the so-called census judgment.[6] The verdict was considered a milestone of data protection as it shaped the "right to informational self-determination". The German Court decision would continue to influence the rise of data protection for decades to come. In 1995, the European Data Protection Directive 95/46/EC was created, reflecting technological advances and introducing new terms including processing, sensitive personal data and consent, among others. The Directive specifically targeted the increasing power imbalance between private corporations and citizens, clarifying that the right to informational self-determination is indeed universal and can be used against anybody.

In 2016, the General Data Protection Regulation (GDPR) was approved by the European Parliament after four years of discussion.[7] The GDPR serves as a blueprint for various data protection acts

2 Warren SD, Brandeis LD. The right to privacy. Harv Law Rev. 1890;4(5):193–220.

3 Universal Declaration of Human Rights. New York: United Nations; 1948 (https://www.un.org/en/universal-declaration-human-rights/).

4 OECD work on privacy. In: Organisation for Economic Co-operation and Development [website]. Paris: OECD Publishing; 2020 (http://www.oecd.org/sti/ieconomy/privacy.htm).

5 Convention 108 and Protocols. In: Council of Europe [website]. Strasbourg: Council of Europe; 2020 (https://www.coe.int/en/web/data-protection/convention108-and-protocol).

6 Abstract of the German Federal Constitutional Court's Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES]. Karlsruhe: Federal Constitutional Court; 1993 (https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html).

7 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). O. J. E. U. 2016, L119:1–88 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679).

around the globe. In 2018, the United Nations enacted the Personal Data Protection and Privacy Principles as the primary source for the protection of personal data by all United Nations institutions.[8]

According to data protection laws globally, personal data means any information relating to an identified or identifiable individual. An identifiable person is one who can be identified, directly or indirectly – in particular, by reference to an identification number (such as a social security number) or by one or more factors specific to their physical, physiological, mental, economic, cultural or social identity (such as surname and first name, date of birth, biometric data, fingerprints and so on).

An important term in this definition is the word "relating", as it implies both that the data are not owned by the data subject (in the sense of a property right) and that the data may equally relate to more than one person. To give an example, the information that a person is colour-blind (something that predominantly affects men) relates equally to the mother as a genetic carrier and to the father of the mother, who will also be colour-blind. Consequently, processing such data based on informed consent may require consent from all data subjects the data relate to. Thus, the "data subject" is any identified or identifiable natural person to whom the personal data refer.

Personal data that have been de-identified, encrypted or pseudonymized but that can be used to re-identify a person remain personal data and fall within the scope of data protection laws.

Personal data that have been rendered anonymous in such a way that the individual is not or is no longer identifiable are no longer considered personal data. For data to be truly anonymized, the anonymization must be irreversible.

2.2 Core principles of data protection in the context of public health

Data protection is principle-driven, building on the core principles enshrined in important documents such as Council of Europe Convention 108, the European Union (EU) Charter of Fundamental Rights[9] and the national constitutions of many countries.

To ensure full compliance with applicable data protection laws and regulations, natural or legal people who process personal data should adhere to the following data protection principles.

- **Fair, lawful and transparent**: personal data shall be processed fairly, lawfully and in a transparent manner in relation to the data subject. In particular, personal data shall not be processed unless permitted by law, based on a preponderant legal interest of the processor or consented to by the data subject.
- **Purpose limitation**: personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- **Accuracy**: personal data shall be accurate and, where necessary, kept up to date.

8 Personal data protection and privacy principles. Geneva: United Nations System; 2018 (https://www.unsystem.org/personal-data-protection-and-privacy-principles).

9 Charter of Fundamental Rights of the European Union. OJEU 2012, C326:391–407 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT).

- **Data minimization**: personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
- **Storage limitation**: personal data processed for any purposes shall not be kept for longer than is necessary for those purposes.
- **Rights of data subjects**: personal data shall be processed in accordance with the rights of data subjects as stipulated by the applicable data protection laws.
- **Integrity and confidentiality**: appropriate physical, technical, legal and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss, alteration or damage to personal data.
- **International transfer of personal data**: personal data shall not be transferred to a third country or international organization unless that country/organization ensures an adequate level of protection of the rights and freedoms of the data subjects in relation to the processing of personal data.[10]

Following these principles ensures that data controllers, such as public health authorities, are capable of demonstrating that they are fully accountable for their activities, and that the data processing is conducted in a fair and balanced way that affects the right to informational self-determination, or the right to privacy, only to the extent necessary to pursue health-related public interest.

Recommended actions

- Develop a holistic understanding of the principles.
- Develop a plan on how to operationalize the principles in the specific setting.
- Develop a long-term plan on how to adhere to these principles systematically.

2.3 The lawful basis of data processing

Regardless of the purpose of processing personal data, such processing is prima facie not permitted unless the data controller has a valid lawful basis to do so (GDPR Article 6). This is enshrined in the first principle of data protection. Six lawful bases for processing are available. No single basis is better or more important than the others – which is most appropriate to use will depend on the purpose of the processing and the relationship with the individual. The lawful basis must be determined prior to the processing, and must be properly documented, as per processing activity. In detail, the six categories are as follows.

- **Consent**: the individual has given clear informed consent for the processing of personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract the data controller has with the individual, or because the data subject has asked steps to be taken before entering into a contract.

10 Further details are available in: Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 (https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition).

- **Legal obligation**: the processing is necessary for compliance with the law (not including contractual obligations).
- **Vital interests**: the processing is necessary to protect someone's life.
- **Public task**: the processing is necessary for the performance of a task in the public interest or as part of an official task or function, and the task or function has a clear basis in law.
- **Legitimate interests**: the processing is necessary for the legitimate interest of a third party, unless there is a good reason to protect the individual's personal data, which overrides legitimate interests; however, this legal basis does not apply if a public authority is processing personal data in order to perform its official tasks.

In the case of data processing activities in the context of health information management tasks, it is obvious that certain types of lawful basis are more likely to apply. Data processing is likely to be carried out based on legal obligation and public tasks; in rare cases, vital interests may apply. Informed consent of the data subject is a critical legal basis: it obviously plays a major role in the case of research activities, but may also have implications for public health purposes that require a high level of completeness of datasets.

Consequently, informed consent of the data subject may not be used if there is a basis in the law (such as a cancer registry), or if there is a clear preponderant public interest (as in the case of a pandemic). The concept of informed consent may only be chosen to the extent the data subject has a "real" choice, and if refusal to consent does not have negative implications for the data subject.[11]

In practice, informed consent of the data subject is often wrongfully applied, as any legal basis will suffice, and informed consent may have a substantive impact on the outcomes of public health activities. Thus, it is often advisable to select an alternative legal basis, but caution is needed, as transparency requirements continue to apply unless specific exemptions kick in.

Recommended actions

- Define the specific legal basis for the data processing.
- Carefully consider the use of informed consent as a legal basis.
- Use the vital interest basis only in exceptional cases if the public health intervention is to the direct benefit of data subjects.
- Document all deliberations and any decisions taken properly.

11 On the legal basis for processing data, a summary is available from: Lawful basis for processing. In: Information Commissioner's Office [website]. Wilmslow: Information Commissioner's Office; 2020 (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/).
On informed consent, see: Guidelines 05/2020 on consent under Regulation 2016/679. In: European Data Protection Board [website]. Brussels: European Data Protection Board; 2020 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en).

2.4 The principle of informed consent

As any data processing needs a legal basis, researchers often turn to the informed consent of data subjects in particular to legitimize the processing of personal data.[12] As noted above, however, informed consent is one of six legal bases; it should only be used in public health if specific conditions are met.

- Consent implies that data subjects have a real choice and control.
- Consent requires a positive opt-in from the data subject: a clear expression of his/her will.
- Consent should be specific and granular – in particular, in relation to the purpose of the processing. Exemptions apply in research: consent to "cancer research" may be specific enough if the data subject is capable of understanding the implications of the consent.
- Broad consent may also be acceptable if the data subject contributes to a public health or research infrastructure, such as a national biobank.[13]

Consent is only appropriate if a public health or medical institution offers data subjects a real choice, and if the data subject is neither directly nor indirectly coerced to consent to the data processing. If the consent is obtained in a medical setting, this is always a critical issue, as refusal to consent may have severe implications on the level of care. Equally, if a data controller cannot – or does not intend to – offer a genuine choice, consent is not appropriate, as the consent process would be misleading and inherently unfair.

Consent must be properly documented; the documentation used should be clear, concise and in a language accessible to the data subjects. Data subjects should have adequate time to consider their choice, and have access to further details and consultation, as deemed necessary. An important part of informed consent is the word "informed", as discussed further in section 2.5 on transparency.

Recommended actions

- Informed consent is not a "short cut": carefully evaluate whether this is the right tool in your processing situation.
- Carefully assess the degree of freedom of the data subject.
- Clearly communicate to the data subject that he/she does indeed have a choice.
- Be granular and specific: avoid broad or blanket consents if possible.

12 Guidelines 05/2020 on consent under Regulation 2016/679. In: European Data Protection Board [website]. Brussels: European Data Protection Board; 2020 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en).

13 Donnelly M, McDonagh M. Health research, consent and the GDPR exemption. Eur J Health Law. 2019;26(2):97–119.

2.5 Transparency

As noted above, one of the core principles of modern data protection laws is the principle of transparency. This links back directly to the landmark decision of the German Court on the census judgment of 1983 (see section 2.1), in which the Court stated:

> *The general right of personality encompasses, based on the notion of self-determination, the power conferred on the individual to, in principle, decide themselves whether and to what extent to disclose aspects of their personal life… If individuals cannot, with sufficient certainty, determine what kind of personal information is known to their environment, and if it is difficult to ascertain what kind of information potential communication partners are privy to, this may seriously impair the freedom to exercise self-determination.*[14]

Thus, transparency is fundamentally and intrinsically linked to the principle of fairness. Transparent processing in a public health context is about being clear, open and honest with data subjects, and therefore requires public health institutions to disclose the basic elements of processing activities.[15]

The provision of clear and concise information in a language that is accessible to the data subject is required, whether the data are collected directly from the data subject or obtained from a third party.

The provision of information is also vital in the case of a change in the purpose of processing – for example, a secondary use of health data – unless specific exemptions apply. Key examples of such exemptions are situations in which the provision of such information proves impossible or would involve a disproportionate effort, or in which the exemption is provided for in law.

As a guide and indicator, public health data controllers may refer to Articles 13 and 14 of the GDPR for the set of information to be provided to the data subject. In addition to direct communication with data subjects via privacy notices or privacy terms, it is also advisable for public health institutions to engage in active dialogue with civil society, and to report regularly to the public on data protection activities.

Recommended actions

- Develop a privacy policy and publish the policy on the website or via other means.
- Make sure you use plain language that is accessible to lay people.
- Make sure you have communication channels in place that enable data subjects to get in touch with you.
- Work proactively with civil society to communicate your data protection concepts and processes.

14 Abstract of the German Federal Constitutional Court's Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES]. Karlsruhe: Federal Constitutional Court; 1993 (https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html).

15 On the concept of transparency under the GDPR, see: Guidelines on transparency under Regulation 2016/679 (wp260rev.01). Brussels: European Commission; 2018 (https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025).

3. The protection of data subjects in data protection law

3.1 The rights of data subjects

Modern data protection laws aim to empower citizens to exercise their rights in a world increasingly dominated by technology companies and other players that process vast amounts of data relating to citizens. The empowerment of citizens is equally important in the context of medical care and similar health-related settings, such as end-of-life decisions.

The rights of data subjects are, as in the medical setting, intrinsically linked to the principle of transparency, as only educated and empowered citizens are capable of exercising their rights. Responsibility for adherence to the rights of data subjects rests with the data controller. As such, the data controller is also obliged to ensure that any data processor – or, in case of a controller-to-controller transfer, any data recipient – honours the rights of data subjects.[16] In detail, these rights are as follows.

- The data subject's **right of access** means a) the right to know whether data concerning them is being processed and b) if so, the right to access such data and to obtain a copy of the data.
- The **right to rectification** means that when personal data are inaccurate, data subjects can require controllers to correct factually inaccurate data.
- The **right to erasure** – in some jurisdictions named the right to be forgotten if personal data have been made public – is a core right to restrict the processing of data and to enforce retention periods.
- The **right to restriction of processing** is, in essence, the right of a citizen to limit the processing of their personal data if they can claim a preponderant right to restricting the processing.
- The **right to be informed** is an underlying right that should be perceived as the cornerstone of data subject rights. Most data protection laws in Europe and elsewhere ask controllers to inform data subjects about several matters, normally in advance and in language that is clear, concise and accessible to a layperson. There are exemptions to the right – for example, in the context of (health and medical) research or other public health activities. Any exemption to the right to be informed, however, must be carefully assessed and documented.

16 For details, see: Voigt P, von dem Bussche A. Rights of data subjects. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; 2017: 141–87.

- The **right to data portability** is a relatively new right in many jurisdictions, and relates to the right to access to data, as it stipulates the right to obtain data relating to a person in a machine-readable format, possibly even in such a way that a citizen can ask a data controller to transfer data to another data controller. The right to data portability is usually limited to data that have been obtained based on the consent of a data subject or a contract with a data subject. It does not apply to processing based on law, and it may not be exercised if it could undermine important public interests, such as public health.
- An important right, in the context of public health activities in particular, is the **data subject's right to object**. This means that data subjects can say they do not want processing of their personal data to be done. While this is an important right in the context of direct marketing or profiling, the right is limited if a public health authority, or another public body, has an overriding interest in the data processing and is processing data for the common good. For example, in a pandemic situation, citizens may not have a right to object to the processing of data if this is necessary for track and trace activities. In such cases, however, the right to object to the processing may effectively oblige public institutions to ensure that only the minimum data needed to accomplish the task are processed.
- The data subject's **right not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning them or similarly significantly affects them, has similar limitations to the right to object in the context of public health activities. Notably, even in an activity that serves the public good, institutions must ensure that the core of the right to informational self-determination is respected fully, and that a data subject is not a mere object of an automatic processing decision.[17]

Adherence to the rights of data subjects is of the utmost importance – in particular, in the context of public health activities, as such compliance by health institutions fosters citizens' trust in the processing activities. If a tracing app in a pandemic situation like COVID-19 ignored the rights of data subjects and paved the way to using such data for secondary purposes, such as the collection of taxes, citizens might refuse to use it. In the online world, trust is the most important currency; once lost, it is almost impossible for public health authorities to regain.[18]

Recommended actions

- Communicate data subjects' rights clearly and effectively.
- Set up processes and points of entry for data subject requests.
- Ensure partnerships with the data subjects, who are the "customers".
- Document data subjects' requests and efforts to serve these.
- Ensure that IT systems facilitate adherence to data subject requests (such as deletion of data).
- Develop a communication strategy on any reasons for turning down data subject requests.

17 For detailed information see: Chapter 6.1 of Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 (https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition).

18 Hodges C. Delivering data protection: trust and ethical culture. Eur Data Prot L Rev. 2018;4(1):65–79.

4. Data protection and public health – legal framework and limitations to the privileged position of health

4.1 Data protection in HISs (including regulatory approaches to health)

Over the last three decades, the level of regulation in the field of data protection and cybersecurity has increased. This guidance focuses less on high-level documents like the EU Charter of Fundamental Rights and instead looks at the level of regulation closer to professionals operating in the field of HISs.

To do this, it is important to distinguish between sector-specific laws regulating the processing of health data, general data protection laws (like the GDPR) and laws that govern the processing of personal data and may have direct or indirect consequences on HISs (such as ePrivacy).

Sector-specific laws are important to the extent that they provide clear guidance on the processing of personal data for health purposes and often serve as a legal basis for processing activities. Such laws may either address specific public health tasks (such as a cancer registry) or govern the use of health information in a clinical/medical setting (as with electronic health records), with subsequent secondary use of data for public health purposes. In fact, data protection calls for development and implementation of such laws, as these help to achieve a maximum level of transparency and democratic legitimacy.

The application of general data protection laws and, in particular, the impact of wider legislation tends to pose significantly greater challenges in the context of HISs. Across general data protection legislation, the processing of personal data for health purposes is privileged. This is the case not only for processing of data for the protection of health ("vital interest") but also for the use of personal data for public health purposes.

For example, Recital 46 of the GDPR states:

> *The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person*[19]*. … Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as, for instance, when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.*

19 "Natural person" follows the definition of a data subject, e.g. in Art 4 (1) GDPR. The antonym would be a "legal person", e.g. a limited liability company or an authority.

Consequently, public health is privileged in terms of the legal basis for data processing (the justification), the scope of processing activities and, in particular, secondary use of personal data for managing HISs.

In day-to-day practice, the implications of further legislation often pose significant problems, including but not limited to ePrivacy (such as website "cookies"), critical infrastructure or IT security regulations. Putting all these laws and regulations into practice, and anticipating the direct and indirect implications in the design and management of HISs, requires a deep understanding of the subject matter and relevant legal expertise.

Professionals in the health information management domain must also be aware that the privileges public health enjoys do not extend to protection of the integrity and availability of data. In brief, serving a laudable purpose – such as protecting public health – does not justify lowering standards of IT security. Such privileges are strictly tied to the specific public health purposes and do not justify secondary use of data for other purposes per se. It is permissible to set up infrastructures that serve secondary use of data, such as registries or biobanks, but each case of secondary use must be scrutinized to protect the interests of data subjects and society.[20]

Recommended actions

- Develop a clear understanding of the sector-specific data protection law.
- Develop a clear understanding of the sector-specific laws that oblige or at least permit the processing of personal data.
- Set up horizon scanning for upcoming changes and how these may affect public health.
- Make sure that IT security standards are strictly adhered to, as public health privileges do not apply to them.

4.2 The "how to" of data protection in HISs (including data protection by design and by default)

Complex and large-scale data processing activities in the public health sector require careful planning and execution. To the extent that such systems require processing of personal data, data protection regulations require data controllers to ensure that they consider privacy and data protection issues at the design phase of any system, service, product or process, and then throughout the lifecycle. Developing and integrating data protection solutions in the early phases of a project identifies any potential problems at an early stage to prevent them in the long run. As such, following a data protection by design and by default approach is part of the accountability of data controllers.[21]

20 For detailed information see: Chapter 9.3 of Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 (https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition).

21 On the concept, see: Guidelines 4/2019 on Article 25 data protection by design and by default. In: European Data Protection Board [website]. Brussels: European Data Protection Board; 2020 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en).

Data protection by default requires controllers to ensure that they only process the data necessary to achieve the specific purpose. This links to the fundamental data protection principles of data minimization and purpose limitation. For the public health sector, this does not lead to a "default to off" solution, as the default design principle again calls for a balancing of the interests at stake, and for limitation of purposes to vital interests such as protection and promotion of health.

Taking the COVID-19 situation as an example, large-scale processing of personal data relating to all citizens may be justifiable and perfectly compliant with the principles, to the extent that such processing is necessary to mitigate the risk of the COVID-19 pandemic. But the principles also call for effective safeguards to ensure that personal data are not used or abused for secondary purposes unless the secondary purpose is equally justifiable (such as research with pseudonymized or anonymized data).

As such, public health institutions must also select partners and service providers carefully – and, in particular, data processors and their subprocessors. IT security and data protection requirements should be part of any relevant tender and procurement process, and the contractual obligations of partners and service providers should mirror all relevant regulatory requirements on the data controller, or any additional requirements a data controller may deem necessary – for example, for the mitigation of reputational risks.

Recommended actions

- Set up a governance process for the development, procurement and implementation of new data processing systems.
- In the light of the processing purpose, develop a strategy on how to minimize implications for data subjects.
- Monitor and audit compliance continuously.
- Select partners carefully, and make sure they adhere to the required standards and demonstrate compliance with data protection requirements.

4.3 Data protection and IT security

While IT security was traditionally concerned with the integrity and availability of data, data protection was associated with the confidentiality of the processing. In recent years, these topics have increasingly merged, and regulatory acts like the GDPR stipulate very stringent data security requirements for data controllers.[22]

This means that controllers (and processors) must have appropriate security measures in place to prevent the personal data they hold being accidentally or deliberately compromised. As such, controllers should bear in mind that while information security is sometimes reduced to cybersecurity (the protection of networks and information systems from attack), it also covers other things like physical and organizational security measures.

22 For details of the security requirements regarding processing of personal data, see: Handbook on security of personal data processing. Athens: European Union Agency for Cybersecurity; 2018 (https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing).

Thus, adequate organizational and technical measures for the protection of personal data are vital to maintain the trust of data subjects in the processing, and will help public health systems to secure public support and compliance of data subjects. Measures may include not only technical measures – such as encryption of data at rest and in transit – but also solid identity and access management or data governance approaches, including classification of data (for example, as strictly confidential/confidential/public). A key aspect of protection is tight management of administration and access rights; public health institutions – and health institutions in general – often fail to implement a strict "need to know" principle.

Regulations like the GDPR may not outline the exact security measures required. Instead, they require controllers to have a level of security that is "appropriate" to the risks presented by the processing. Public health authorities and other actors in the sector need to consider this in relation to the latest developments and costs of implementation, as well as the nature, scope, context and purpose of the processing.

Bearing in mind that the public health sector is often tasked with processing sensitive personal data, such as data relating to health and physical well-being, data subjects will expect a very high level of data security in such operations. Having said that, non-availability of funds for data security measures is no excuse, to the extent that those measures are necessary to achieve an "appropriate" level of protection.

An important topic is the handling of data breaches – breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.[23] This includes breaches that are the result of both accidental and deliberate action. Institutions of any size or setup are easily overwhelmed by a data breach situation. As such, public health institutions are advised to plan for this eventuality, possibly even by conducting a cyber incident simulation. A data breach plan – with clear allocation of tasks and responsibilities – is needed, including a data breach communication strategy.

An important tool is regular penetration tests, carried out by an independent third party: in simple terms, a data controller should invite "ethical hackers" to test the weaknesses of the system. Many countries have IT security or cybersecurity agencies that support public health institutions in setting up such concepts. For institutions that serve operational purposes, a disaster recovery plan is equally critical and strictly required.

Recommended actions

- Define and document the technical and operational measures.
- Define and monitor IT security requirements, ideally based on best practices like the International Organization for Standardization (ISO) 270XX series.
- Set up and maintain identity and access management, ensuring that administrator rights are limited and that a "need to know" concept is followed.
- Ensure that data are always encrypted, both in transit and at rest.

23 See the guidance at: Personal data breaches. Wilmslow: Information Commissioner's Office; 2020 (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/?q=data+breach).

- If applicable, develop a security strategy for the use of cloud computing, in particular the use of public clouds.
- Assess and monitor IT security regularly – for example, by conducting third-party penetration tests.
- Develop a data breach procedure and communication strategy.
- Develop a disaster recovery plan as needed.

5. Processing of personal data in public health systems – guardrails for primary and secondary use of data

5.1 Use of personal data for management of HISs (including the concept of secondary use)

For the purpose of this document, the term "HIS" refers to a system designed to manage health care data in a wider sense. This includes systems that collect, store, manage and transmit a patient's electronic health records, a hospital's operational management or a system supporting health care policy decisions. Obviously, different dimensions of HISs pose significantly different and heterogeneous data protection challenges.[24] While the temporary non-availability of data may be negligible in the context of health care policy-making, it may have catastrophic consequences in a hospital setting.

This guidance focuses on the management of HISs and the policy-making dimension. Such data may often be aggregated or anonymized, and may therefore not fall under data protection regulations. In terms of public health policy-making, the secondary use of data is of utmost importance. If possible, personal data should be aggregated or anonymized at source, minimizing data protection risks and maintaining the control of the initial data controller. Depending on the use of the data – for example, in cancer registries or biobanks – aggregation or anonymization at source may have an impact on the quality, requiring a centralized approach to processing. Personal datasets and aggregated or anonymized data should be kept separate, at least by means of a logical separation, and ideally in physically separated IT systems.

Infrastructure should be set up as needed, based on a concept of pseudonymization (rather than anonymization),[25] enabling public health data controllers to go back to an individual data subject, to the extent that this is to the direct benefit of the data subject. An example might be processing of data relating to environmental determinants of health – such as research on asbestos in a specific community or industry.[26]

24 For more details, see: Michelsen K, Brand H, Achterberg P, Wilkinson J. Promoting better integration of health information systems: best practices and challenges. Copenhagen: WHO Regional Office for Europe; 2015 (Health Evidence Network Synthesis Report, No. 40; https://www.euro.who.int/en/publications/abstracts/promoting-better-integration-of-health-information-systems-best-practices-and-challenges).

25 Hintze M, El Emam K. Comparing the benefits of pseudonymisation and anonymisation under the GDPR. J Data Protect Priv. 2018;2(2):145–58.

26 For example, see: Visonà SD, Villani s, Manzoni F, Chen T, Ardissino G, Russo F et al. Impact of asbestos on public health: a retrospective study on a series of subjects with occupational and non-occupational exposure to asbestos during the activity of Fibronit plant (Broni, Italy); J Public Health Res. 2018;7(3):1519. doi:10.4081/jphr.2018.1519.

Recommended actions

- Anonymize or aggregate data at source if possible.
- Make sure raw data and anonymized or aggregated data are at least logically (and ideally physically) separated.
- Use pseudonymized data if the outcomes of the data processing may benefit individuals.
- For registries or biobanks, develop a comprehensive security concept.

5.2 Personal data and health research (including the concept of secondary use)

One of the core principles of data protection is the principle of purpose limitation, as data controllers need to specify the exact purpose prior to starting processing activities. In the case of health data, the purpose limitation principle is not absolute, as secondary use of health data is often vital for management and improvement of public health systems. As such, health-related data, including data on various determinants of health, are an important resource for policy-making, health systems management and research.[27] Research is privileged, and the freedom of research (and researchers) is a constitutional fundamental right in many countries, and in various multinational policy documents.[28]

To the extent that research is the primary purpose of the data processing, and such data have been obtained with the informed consent of the data subjects, the consent limits the ability to use data for further purposes if these purposes are not strictly related to the primary purpose. In practice, a more complex situation is secondary use of data for public health purposes – for example, data that have been processed initially in a medical setting.[29]

Some laws and regulations are very specific about the legal safeguards required, and in the case of the GDPR call on Member States to regulate the issue in more detail in national law, as health itself is primarily outside the competence of the EU. Irrespective of the specificities of the GDPR, secondary use is permitted if such use is not incompatible with the primary purpose, if there is a lawful basis and if the processing is proportionate and necessary steps are undertaken to maintain the security of the data.[30] To the greatest extent possible, data protection calls for pseudonymization, masking or even anonymization of data if such data still serve a public health purpose. It would be an infringement of data protection law if the data were kept in their original shape and form just as a matter of convenience, or to minimize processing efforts.

27 Taylor MJ, Whitton T. Public interest, health research and data protection law: establishing a legitimate trade-off between individual control and research access to health data. Laws. 2020;9(1):6.

28 Chassang G. The impact of the EU General Data Protection Regulation on scientific research. Ecancermedicalscience. 2017;11:709. doi:10.3332/ecancer.2017.709. For an interesting perspective from Canada, see: Steeves V. Data protection and the promotion of health research. Healthc Policy. 2007;2(3):26–38.

29 Peloquin D, DiMaio M, Bierer B, Barnes M. Disruptive and avoidable: GDPR challenges to secondary research uses of data. Eur J Hum Genet. 2020;28:697–705. doi:10.1038/s41431-020-0596-x.

30 Chico V. The impact of the General Data Protection Regulation on health research. Br Med Bull. 2018;128(1):109–18. doi:10.1093/bmb/ldy038.

Due to the heterogeneity of the regulatory landscape in the WHO European Region, a detailed assessment is needed on a case-by-case basis before embarking on a specific research project that requires secondary use. Again, it is of utmost importance to document the deliberations carefully, and to be as transparent as possible towards the data subjects and other relevant stakeholders. Specific requirements may apply if the activities require transfers of data across borders or to a multinational organization.

In the case of processing of data for public health and research, certain limitations to the rights of data subjects may apply. Public health workers and researchers are encouraged to make use of these exemptions only as far as strictly necessary. Equally, exemptions may apply in terms of the retention/deletion of data, as new – and therefore different – retention periods may apply.

Recommended actions

- Make sure research activities are separated from policy-oriented data processing activities.
- Separate IT infrastructure for research from operational data processing activities.
- Encourage researchers to work with data, and educate them about research privileges.
- Assess the legal framework carefully for cross-border research activities.
- Document research activities properly – for example, in terms of the justification for secondary use and the retention of data for research purposes.

5.3 Finding the balance between data protection and public health

As noted above, personal data is not a "property" of the data subject, as it relates to a person but may equally relate to others. Laws, regulations and courts also note that individuals are part of society; they interact with society and are subject to various legal interests that may equally require protection. In the context of public health and the management of HISs, the right to health in particular is a core fundamental right that is globally recognized as one of the most important rights of individuals.

The right to health was first articulated in the WHO Constitution of 1946, which states that "the enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being". The preamble to the Constitution defines health as "a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity".[31]

The right to health is an inclusive right, extending not only to timely and appropriate health care but also to the underlying determinants of health, such as access to safe and potable water and adequate sanitation, healthy occupational and environmental conditions, and access to health-related education and information, including on sexual and reproductive health. While the right to health is a fundamental right that protects the individual, it also serves as a justification for activities of state agencies and other stakeholders that aim to foster the right to health. Thus, the creation

31 Constitution of the World Health Organization. Geneva: World Health Organization; 1946 (https://www.who.int/about/who-we-are/constitution).

and maintenance of an HIS, which supports access to health information and the management of health systems, is a legally recognized interest that needs to be balanced with data protection.

Balancing in this sense should not be perceived as a yes or no decision, but rather as an attempt to protect both interests and the underlying fundamental rights in the best possible way.[32] Consequently, all public health actors should define the public health interest they want to pursue (the "purpose"), and then identify the methods and means that pose the least possible threat to the right to informational self-determination. In rare cases, the analysis may show that the public health interest does not justify curtailment of the right to informational self-determination; in other scenarios – such as during a pandemic – even severe implications for data protection may be legally acceptable. Notably, the concept of purpose is of the utmost importance in this context, as the processing of data from a COVID-19 contact-tracing application may be acceptable for the purpose of protecting public health, but at the same time may not be acceptable for law enforcement activities targeting petty crime.

The balancing of interests at stake – and in particular the accordance of fundamental rights – equally needs to be reflected in the policy-making processes, including drafting of laws and other pieces of legislation. Much of this is due process, as the decisions underlying such balancing require judgements, often under conditions of uncertainty (for example, during a situation like COVID-19, as it is unclear a priori how a pandemic may unfold). Again, it is crucial to be transparent in deliberations and to communicate properly to citizens and other actors of civil society.

The process of balancing the interests and fundamental rights at stake is not an easy one, and there is no universal recipe. Achieving an accordance of the rights requires proper documentation and transparency towards all relevant stakeholders, including the wider public and data subjects affected by the activities. This process is also important to determine whether a data processing activity may require the consent of the data subject or whether a legitimate, preponderant legal interest justifies the processing of personal data.

Recommended actions

- Educate public health professionals on how to strike a balance between the fundamental rights at stake.
- Engage with civil society regarding the value of data processing for public health activities.
- Set up ethical and legal benchmarks for exceptional situations, such as a pandemic situation like COVID-19.

32 Dworkin R. A matter of principle. Cambridge, MA: Harvard University Press; 1985.

6. Building a data protection management system in public health

6.1 Operationalizing data protection in HISs

Data protection laws around the world pursue a risk- and process-oriented approach to ensure the confidentiality, integrity and availability of data and the resilience of systems. This requires a periodic process to review the effectiveness of the security measures and their continuous improvement. Data protection is not a one-off activity, but a task that needs to be embedded into all activities relating to the management of HISs. Equally, data protection is a task and responsibility of everyone involved in data processing, and should not be assigned exclusively to a data protection officer or data governance department.

An important tool to ensure that all relevant stakeholders in an organization assess data protection requirements is the data protection impact assessment (DPIA). This formal process and documentation tool is widely used for high-risk data processing activities, and various data protection authorities and other stakeholders provide templates. A DPIA is recommended prior to the going live of a new IT system or processing activity.[33]

Data protection officers should be in post to guide the organization, but the day-to-day responsibility for compliance with data protection laws rests with the data controller, as the entity in charge of data processing.

As such, data protection requires adequate resources, continuous training and support from the highest management level. The data controller should also ensure that relevant data protection audit capacities are available, and should be able to support audits of data protection authorities. A data protection audit is defined as a systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with an organization's data protection policies and procedures, and whether this processing meets the requirements of the applicable regulatory framework.[34] The audit programme should lead to a continuous improvement plan, and may lead to the completion of industry certification programmes, such as ISO 27001 or ISO 27701.[35]

33 See the guidance at: Data protection impact assessments. Wilmslow: Information Commissioner's Office; 2020 (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).

34 See the guidance of the French data protection authority: What you should know about our standard on data processing audits. Paris: Commission Nationale de l'Informatique et des Libertés; 2020 (https://www.cnil.fr/en/what-you-should-know-about-our-standard-data-processing-audits).

35 Lachaud E. The General Data Protection Regulation and the rise of certification as a regulatory instrument; Comput Law Secur Rev. 2018;34(2):244–56.

Recommended actions

- Set up a risk management system for data protection, covering various dimensions of risk such as financial risk or a reputational risk.
- Ensure support from the highest management level of the institution.
- Report to the highest management level regularly, and prepare regular (annual or similar) reports on data protection.
- Set up mid- and long-term financial planning for data protection resources.
- Follow internationally recognized standards such as ISO 27001 and audit compliance with these frameworks.
- Conduct a DPIA for high-risk activities.
- If the institution does not adhere to an overall, holistic data protection framework, start small and develop a concept for the team or department.

6.2 Education and empowerment

Data protection is an important component of the human-centric approach to technology and a compass for the use of technology in the digital transition of economies and policy-making. In a public health system increasingly based on the processing of personal data, the legal safeguards highlighted above are an essential tool to ensure that individuals have better control over their personal data and that these data are processed for a legitimate purpose, in a lawful, fair and transparent way. As data protection must be embedded into the design and execution of public health programmes, this requires education and empowerment of both citizens and public health professionals.

Data competence, including governance of data processing and protection of personal data, must become an integral part of the qualification of public health professionals working on HISs.[36] Such education must be based on the principles described, but should also cover the applicable regulatory framework. An important element is the continuous qualification of professionals who have already passed the period of academic education. Workshops, hands-on exercises and problem-based learning are needed to break the barriers between public health and data protection.

Continuous education is also vital to enable public health professionals to keep up with the pace of implementation of new technologies, such as cloud computing or blockchain-based systems. Empowerment is needed to be capable of applying the principles of data protection correctly in the ever-changing technological landscape.

36 For conceptual issues of embedding data protection in training and education programmes, see: González Fuster G, Kloza D. The European handbook for teaching privacy and data protection at schools. Brussels: European Commission; 2016 (http://arcades-project.eu/index.php/deliverables).

Recommended actions

- Ensure that data protection becomes an integral part of public health education.
- Develop continuous learning offerings for data protection.
- Set up a training plan for the institution.
- Develop refresher courses or problem-based learning techniques that address the specific needs of the institution.
- Support the introduction of new technologies or data processing systems by relevant education programmes.

6.3 External oversight, internal control and enforcement measures

As part of the accountability principle, data protection requires any data controller to take responsibility for their processing activities and for how they comply with data protection principles. Having appropriate measures and records in place to demonstrate compliance is critical. Another key requirement is internal and external control; this control structure may take a different shape or form depending on the applicable law. Various data protection laws lay down that the position of a data protection officer or privacy officer should be established. This is an independent role in an organization that provides advice to the data controller, maintains the records of the processing activities and serves as a point of entry for data subjects and authorities.[37]

The data protection officer also leads audit activities, both in-house and into third parties that process data on behalf of the data controller. The audit function of the data protection officer is regularly supported by internal or external IT audit capabilities. Importantly, a data protection officer should not have any conflict of interest, and should report to the highest management level of the organization.

The majority of countries in the WHO European Region have created specific data protection authorities, and some differentiate between authorities overseeing public or private institutions. Using its statutory powers, a data protection authority will examine complaints from data subjects in relation to potential infringements of data protection law, conduct enquiries and investigations regarding infringements of data protection legislation and take enforcement action where necessary, and promote awareness regarding the rights of data subjects to have their personal information protected under applicable data protection law.

Public health authorities should bear in mind that the risks associated with data protection infringements are manifold, with reputational damage the primary risk. In addition, public health authorities and research institutes can be subject to monetary fines (in the case of the GDPR up to €20 million) or to an injunction or call for remedy by a data protection authority.[38] Clearly, this requires solid data protection risk management at any larger public health institution – as such, expert knowledge is required at the interface between compliance, IT and data protection.

37 For more details see: Guidelines on data protection officers ('DPOs'). Brussels: European Commission; 2017 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048).

38 Voigt P, von dem Bussche A. Enforcement and fines under the GDPR. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; 2017: 201–17.

One important way to address such risk is to adhere to recognized standards and certificates, such as the ISO 27701 for data protection management systems. As pursuing such certificates can be cumbersome and requires the allocation of adequate resources, any data controller should set up an internal data protection control system that is adequate and corresponds to the data protection risks of the organization.

Recommended actions

- Appoint a data protection officer – someone independent and knowledgeable.
- Set up an internal audit function for IT security and data protection.
- Proactively engage with data protection authorities and civil society.
- Collaborate with partners, both within the country and abroad, to exchange best practices.
- Document activities properly to serve the accountability principle.

7. Conclusions

Compliance with data protection requirements is a challenge for the entire public health community, and specifically for all institutions actively involved in the management of HISs. Notably, the gradually increasing regulatory pressure over the last decades is forcing the public health sector to adjust its policies and practices regarding processing of personal data. It is important to demystify data protection and to provide guidance on how to set up public health measures that comply fully and serve the community. Safeguarding data protection in public health involves new and significant challenges, as technological advances expand the frontiers of areas such as surveillance, Big Data and cloud data storage. Consequently, it is of great importance that public health institutions are equipped to balance the different fundamental rights at stake, and to apply the principles of data protection.

Data protection is not rocket science: it requires legal and technical artisanship, the allocation of adequate resources and the training of all professionals involved in the processing of personal data. Data protection is not a one-off activity but a continuous effort that is based on an institutional vision, a governance concept and a willingness to be accountable. This accountability, based on a thorough risk assessment, builds on the documentation of data protection activities and persistent internal and external oversight.

While doing justice to all these aspects and requirements may sound overwhelming at first, the most important thing is to get started, even if the start is less ambitious and more a piece-meal approach than a holistic concept.

8. Glossary

Anonymous data	Recital 26 of the GDPR defines anonymous information as "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".
Data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
Data controller	The data controller is 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 for its nomination may be provided for by Union or Member State law.
Data processing	Data processing means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data processor	The data processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
Data protection authority	A data protection authority is an independent public authority established by the government.
Data subject	The data subject is the identified or identifiable natural person to which the personal data refer.

Personal data	Personal data 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Pseudonymization	Pseudonymization is defined within the GDPR (Art 4 (3b)) as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual".

World Health Organization
REGIONAL OFFICE FOR Europe

The WHO Regional Office for Europe

The World Health Organization (WHO) is a specialized agency of the United Nations created in 1948 with the primary responsibility for international health matters and public health. The WHO Regional Office for Europe is one of six regional offices throughout the world, each with its own programme geared to the particular health conditions of the countries it serves.

Member States

Albania
Andorra
Armenia
Austria
Azerbaijan
Belarus
Belgium
Bosnia and Herzegovina
Bulgaria
Croatia
Cyprus
Czechia
Denmark
Estonia
Finland
France
Georgia
Germany
Greece
Hungary
Iceland
Ireland
Israel
Italy
Kazakhstan
Kyrgyzstan
Latvia
Lithuania
Luxembourg
Malta
Monaco
Montenegro
Netherlands
North Macedonia
Norway
Poland
Portugal
Republic of Moldova
Romania
Russian Federation
San Marino
Serbia
Slovakia
Slovenia
Spain
Sweden
Switzerland
Tajikistan
Turkey
Turkmenistan
Ukraine
United Kingdom
Uzbekistan

World Health Organization
Regional Office for Europe
UN City, Marmorvej 51
DK-2100, Copenhagen Ø, Denmark
Tel: +45 45 33 70 00
Fax: +45 45 33 70 01
Email: eurocontact@who.int
Website: www.euro.who.int