Patrycja Dąbrowska-Kłosińska[*]

Tracing Individuals under the EU Regime on Serious, Cross-border Health Threats: An Appraisal of the System of Personal Data Protection

This is a draft version of an article prepared to be published in European Journal of Risk Regulation, Special Issue, December 2017. Please consult the Journal for the final version.

Abstract:
The article tackles the issue of personal data protection in case of tracing (looking for) individual persons who have been exposed to health risks pursuant to the EU Decision 1082/2013 on Serious, Cross-border Health Threats. This problem exemplifies just one among many challenges of the health-security nexus in the EU. That is, it relates to a certain trade-off between the limitation of individual rights and securing populations' safety. The text appraises the safeguards for the (lawful) limitation of the right to data protection after an in-depth examination of the provisions of the Health Threats Decision, its implementing measures, the reports on its operation, and in light of the general EU Data Protection Laws. From a regulatory standpoint, it concludes that a number of improvements are needed because of the incompleteness, and the insufficient coherence and transparency of the EU regime for health threats. The established shortcomings are, at least in part, caused by the new EU "integrated approach" to health and security. In effect, an overall philosophy of reforms of public health policy in the name of "all-hazards security" applied in the Health Threats Decision can result in reducing of the adequate level of protection of individuals' personal data.

Keywords: Right to personal data protection, EU public health law, Medical privacy, EU health governance, EU Decision 1082/2013 on Health Threats

I. Introduction

On 25 May 2007, the Italian health authorities reported a case of extensively drug-resistant tuberculosis (XDR-TB) through the EU Early Warning and Response System for infectious diseases.[1] A person concerned, an American citizen, went travelling in Europe despite the warning notice of the federal Centre for Disease Control and Prevention. First, he flew on a long-haul flight between Atlanta (U.S.) and Paris to marry in Rome and spend his honey-moon in Greece; next, he returned to America on a flight from Prague to Montreal (Canada) to re-enter the U.S. by car through the north-east border. Finally, he was halted and forced to treatment in New York. The "Tuberculosis Traveller", as nick-named by alerted media which

[*] PhD, Assistant Professor at the Centre for Europe, University of Warsaw. I am grateful to an anonymous reviewer for the helpful comments on an earlier draft. All omissions remain mine.

[1] See Report on Operation of the Early Warning and Response System (EWRS) of the Community Network for the epidemiological surveillance and control of communicable diseases during 2006 and 2007 (The 2009 Report) (COM(2009) 228 final) 5-6.

did not hesitate to communicate his real name worldwide, alarmed authorities on both sides of the Atlantic and immediately caused tracing of co-travellers on transatlantic flights. Eventually, his story prompted modifications of the U.S. federal quarantine law.[2] In the EU, the event provoked several meetings of the Commission with the affected Member States, the European Centre for Disease Control and Prevention ("ECDC"), the World Health Organisation ("WHO"), the U.S., Canada and the Commission's Delegations in those states, in order to co-ordinate an adequate response. It also "*highlighted the need to strengthen the existing mechanism for contact tracing*" and added to the debate on the future reform of the control of infectious diseases and epidemiological surveillance in the EU.[3]

Apart from the regulatory effects, the above story shows nicely that tracing individuals in case of exposure to a health risk regards the protection of their fundamental rights and the exercise of powers of health authorities at the expense of those rights. One of the rights which is particularly vulnerable to infringements in this context is the personal data protection, including sensitive health data, which are shared among public authorities who try either to find a source of a health threat or to protect those who can be affected, and the population at large, from its spreading. That is why, the application of any measures which involve sharing of personal data in the name of public health security requires strict material and procedural safeguards to ensure an adequate protection of rights of all affected individuals (data subjects).[4] The more so, as the public health security agenda assumes that the trade-off between the limitation of individual rights (disclosure of personal data) and a better protection of public health and populations' safety is unavoidable.[5] But for this reason it is crucial to ask: is it a fair trade off? Are there sufficient safeguards for lawful limitations of individual rights provided in regulatory acts?

Against this background, the objective of this article is a critical appraisal of the system of rules and safeguards for personal data protection in the EU regime on serious cross-border health threats established by the Decision 1082/2013 (Health Threats Decision). In order to pursue this aim, section 2 explores the EU tools allowing for exchange of personal (health) data to manage public health and the legal basis for processing of those data under the general EU Data Protection Laws; and section 3 moves to examine the legal safeguards for the

[2] Hilary Fallow, "Reforming Federal Quarantine Law in the Wake of Andrew Speaker: 'The Tuberculosis Traveller'" (2008) 25 *Journal of Contemporary Health Law & Policy* 83.
[3] Proposal for a Decision on serious cross-border threats to health (COM(2011) 866 final) point 5.4.
[4] See also: Wendy Mariner, George Annas and Wendy Parmet, "Pandemic Preparedness; A Return to the Rule of Law" (2009) 1 *Drexel Law Review* 341; Benjamin Goold, Liora Lazarus, *Security and Human Rights* (Hart Publishing, 2007).
[5] See further Hylke Dijkstra and Anniek De Ruijter in this volume.

protection of those data pursuant to Health Threats Decision. The analysis allows to specify the shortcomings of the present EU regime for prevention of health threats in section 4 (i.e., the current incompleteness, insufficient coherence and transparency). The shortcomings, are at least in part, caused by the EU "integrated approach" to health and security applied in the Health Threats Decision.[6] As a consequence, those phenomena can result in reducing of the adequate level of protection of individuals' personal data. In conclusions, I put forward some suggestions for improvements and consider the perspectives for data protection under EU regime for health threats in case of reforms of public health policy in the name of "all-hazards security".

II. Exchange of Personal Data as a Part of the EU Response to Health Threats

In 2013, the EU adopted a Decision 1082/2013 on Serious Cross-border Health Threats (Health Threats Decision) which aims at preparing and responding to serious health threats (including diseases, bioterrorist, chemical or environmental events); and which restructures and replaces the previous regime on control of communicable diseases.[7] The Decision – formally a public health measure based on Article 168 TFEU – is an exemplary illustration of the "integrated approach" to health and security in the EU. It consolidated the existing tools and powers of institutional actors (e.g. Health Security Committee); introduced some new instruments (e.g. a joint procurement of medicines); and expanded the scope of the previous regime.[8] The act merged the earlier separate policies and programmes (chemical agents, bio-preparedness, and public health) to provide for a co-ordinated, and wider "all-hazards" approach to public health security at the Union level.[9] This revised EU approach was linked to the security agenda within the new global framework for public health security as created by the WHO International Health Regulations in 2005.[10]

A key novelty of the Reformed EU regime for control and prevention from serious, cross-border health threats is the "all-hazards approach". As signalled above, it means that the scope

[6] See Anniek de Ruijter, "Mixing EU Security and Public Health in the Health Threats Decision" in Anniek de Ruijter and Maria Weimer (eds), *EU Risk Regulation, Expert and Executive Power* (Hart Publishing, 2017).
[7] Decision 1082/2013/EU on serious cross-border threats to health [2013] OJ L 293/1 (Health Threats Decision) which repealed Decision 2119/98/EC setting up a network for the epidemiological surveillance and control of communicable diseases in the Community [1998] OJ L 268/1 (Old Surveillance Decision).
[8] Mark Flear, *Governing Public Health: EU Law, Regulation and Biopolitics* (Blumsbury Publishing, 2015) 144.
[9] Recital 3 and 6 of the Preamble, Health Threats Decision. See also Council Conclusions on lessons learned from the A/H1N1 pandemic – health security in the European Union (doc. ref. 12665/10, 13 September 2010) and Presidency Conclusions on Bioterrorism, 15 November 2001, doc. ref. 13826/01.
[10] Cf. Andrew Lakoff, "Two Regimes of Global Health" (2010) 1 *Humanity* 59; and David Fidler, "From International Sanitary Conventions to Global Health Security: The New IHR" (2005) 4 *Chinese Journal of Int'l Law*.

of application of the regime was broadened: it used to apply to communicable diseases only, and now, it applies to a wide range of "serious threats" to health.[11] The material scope of a notion „serious threat" encompasses: biological threats, including contagious diseases, antimicrobial resistance and healthcare-associated infections (e.g. post-hospital treatment viral infections), bio-toxins, or other harmful biological agents, as well as threats of chemical, environmental and unknown origin.[12] Risks of threats concerned can be natural or man-made, e.g. bio-terrorism.[13] Those events can simultaneously amount to "a public health emergency of international concern" pursuant to the WHO International Health Regulations – in this sense, the Health Threats Decision ensures the appropriate link between the EU and international regimes.[14]

Further, the Health Threats Decision introduces several strategic methods for responding to those threats.[15] They concern multi-faceted aspects of reacting to potential "all-hazards" catastrophes, that is: preparedness planning and response coordination; joint procurement of medicines; information exchange, epidemiological surveillance and monitoring; and finally, recognition of emergency situations.[16] The general methods are further applied through the respective institutions and tools operating at the EU level pursuant to the provisions of the Health Threats Decision, for example, "a network for the epidemiological surveillance" (Article 6); "ad hoc monitoring" (Article 7); "Early Warning and Response System" (Article 8); and "an alert notification" which can lead to individual contact tracing (Article 9).[17]

In some cases, the measures can entail sharing of personal information between responsible authorities in the aim of prevention of the public health danger from all types of threats, and eventually result in a (lawful) restriction of the right to personal data protection. Those measures will be analysed closer in the following parts in order to explain their normative character and practical operation. It will allow for the following appraisal of the data

[11] Opinion of the European Data Protection Supervisor on the proposal for a decision of the European Parliament and of the Council on serious cross-border threats to health, Executive summary [2012] OJ C 197/21, point 4.
[12] Art. 2 para. 1; Art. 3 point g), Health Threats Decision.
[13] See point 4 of the Preamble, Health Threats Decision; Frida Kuhlau, "Countering Bio-Threats: EU Instruments for Managing Biological Materials, Technology and Knowledge", (2007) 19 *SIPRI Policy Paper* 1.
[14] Art. 2 para. 1, Art. 4 para. 2, Health Threats Decision, in relation to Art. 1, para. 1, International Health Regulations, http://www.who.int/emergencies/en/ (accessed 12 May 2017).
[15] See Stefan Brem, Stéphane Dubois, "Different perceptions, similar reactions: Biopreparedness in the European Union" in Peter Katona et al. (eds), *Global Biosecurity Threats and Responses* (Oxon-New York 2010) 137-156.
[16] See Art. 4-12, Health Threats Decision. See also Filippa Lentzos, Nicolas Rose, "Governing insecurity: contingency planning, protection, resilience", 38 *Economy and Society* 230.
[17] The text focuses on the measures which may involve personal data exchange. The tools which collect anonymised data for mandatory reporting are of no direct concern here.

protection safeguards, and at the same time, guide the reader through the considerable complexity of the applicable regulatory framework.[18]

[18] See also Marcus Frischhut and Scott Greer, "EU public health law and policy – communicable diseases" in Tamara Hervey et al. (eds), *Research Handbook on EU Health Law and Policy* (Edward Elgar 2017) 315-331.

1. EWRS and Article 9 Alert Notification of Threats: Actors, Scope, and Operation

The Early Warning and Response System ("EWRS") for serious, cross-border health threats, which replaced the preceding mechanism that had been established under the Old Surveillance Decision applicable to infectious diseases only, is now based on Article 8 of the Health Threats Decision. EWRS constitutes a constant communication channel between the Commission and competent authorities ("CAs") of Member States which is administered and coordinated by the European Centre for Disease Prevention and Control in Stockholm ("ECDC").[19]

The key obligation of the EWRS CAs is to "*notify an alert in the EWRS where the emergence or development of a serious cross-border threat to health*" fulfils the normative criteria cumulatively (the statutory conditions).[20] It has to be done within 24 hours since authorities become aware of a threat.[21] They are obliged to warn the EWRS partners in case of risk to health when: (1) "*more than one Member State*" is concerned (geographical criterion); (2) there is a high probability of risk based on either of four alternative indicators: an unusual character of event, a level of morbidity/mortality; pace of spreading; or an overall extent (risk factor); (3)"*it requires or may require*" a coordinated response at the EU level (the subsidiarity principle).[22] The understanding of a "cross-border" and "serious" character of a threat is defined broadly as "a life-threatening or otherwise serious hazard to health" which spreads or entails a significant risk of spreading across the Member States, and thus requires EU level response.

The scope of information which authorities are obliged to provide in Article 9 alert is the widest possible to include "*any available relevant information in their possession that may be useful for coordinating the response*."[23] The Health Threats Decision contains the exemplary enumeration of information which must be provided for the full characterisation of a health threat event and an organisation of an appropriate response. For example: type and origin of an (pathogenic) agent, the date and place of the incident or outbreak, means of transmission,

[19] Point 5 of the Preamble, Art. 6 and 9, Health Threats Decision; and Art. 8, para. 1, Regulation (EC) No 851/2004 establishing a European Centre for Disease Prevention and Control (ECDC Regulation) [2004] OJ L 142/1. See <http://ecdc.europa.eu/en/aboutus/what-we-do/surveillance/Pages/index.aspx> (accessed 10 May 2017).
[20] Art. 9 para. 1, Health Threats Decision. See also Art. 4, Regulation 851/2004.
[21] Art. 2, para. 1, Commission Implementing Decision (EU) 2017/253 laying down procedures for the notification of alerts as part of the early warning and response system established in relation to serious cross-border threats to health and for the information exchange, consultation and coordination of responses to such threats pursuant to Health Threats Decision [2017] OJ L 37/23 (Implementing Decision on Alerts).
[22] Art. 9 para. 1, points a-c, Health Threats Decision.
[23] Art. 9, para. 3, Health Threats Decision.

methods of detection, toxicological data, risks, implemented/planned public health measures, and – what is the most interesting for the purposes of this text – "*personal data necessary for the purpose of contact tracing*" which can also mean health personal data.[24]

From the perspective of data protection, it needs to be explained that the transmission of information within EWRS is carried out via two channels. The first one, the general information channel, enables CAs concerned to send an alert message on health threats under obligatory notification to all the national public health contact points in the EU, the Commission, ECDC and WHO. The actors empowered to participate in EWRS include: the Unit responsible for crisis management and preparedness in health within the Commission's Directorate General for Health (SANTE), the national public health authorities designated to EWRS by the Member States governments ("EWRS CAs"), and delegated ECDC and WHO representatives.[25]

The second communication channel of EWRS is the so-called selective-messaging channel. It is used in case of exchange of personal information or personal health data when a contact tracing procedure is applied. The selective-messaging functionality allows communication between the national CAs concerned only and it was created especially as a specific measure to guarantee and implement the personal data protection.[26] The horizontal design of EWRS and its electronic tools warrant that all the responsible actors receive the information immediately and simultaneously, and if the protection of personal data so require, that those data are exchanged only between the interested states.[27] So, technically, EWRS is an electronic platform with an access limited to international/EU/national competent institutions because of the possible processing of either personal data or other sensitive information about public health security. The process of sending alerts and exchange of any information is always undertaken via designed electronic means. The details of the EWRS functioning, and its operational procedures, are regulated, or awaiting regulation, in the implementing acts of the Commission.[28]

Finally, Article 9 alert notification is a *sui generis* EU administrative act which can cause several legal effects both at the EU and national level. For example, it can trigger a risk

[24] Art. 9 para. 3, points i)-j). See EU Agency for Fundamental Rights and Council for Europe, *Handbook on European data protection law* (Luxembourg Publications Office of the European Union, 2nd edn, 2014) 92.
[25] <https://ewrs.ecdc.europa.eu/> (accessed 12 May 2017).
[26] See Commission Recommendation 2012/73/UE on data protection guidelines for the Early Warning and Response System [2012] OJ L 36/31, point 5 (Old Commission Data Protection Guidelines).
[27] Art. 16 para. 3, Health Threats Decision.
[28] See Art. 8 and 20, Health Threats Decision, and the EU implementing legislation available at: <http://ec.europa.eu/health/communicable_diseases/early_warning/comm_legislation_en.htm> (accessed 10 May 2017).

assessment by ECDC (or other EU agency), an obligation to assess risks, co-ordinate actions and manage risks by national CAs, and moreover, the ad hoc monitoring and individual contact tracing means, which can also entail the exchange of personal data.[29]

2. *Ad hoc* Monitoring

The Health Threats Decision introduced a new tool, named "*ad hoc* monitoring", but so far little has been known about its application and practical operation. The regulation in the Decision is rather laconic (Article 7). Decision says that it applies to health threats other than infectious diseases, that is, in case of bio-toxic, chemical, environmental or unknown danger. It is activated following the Article 9 alert notification concerning one of those health threats. Member States and the Commission are then required to inform each other about the development of those threats at the national level and on the basis of information from national, internal monitoring systems.[30] Pursuant to Article 7, para. 2, the mandatory information "*shall include, in particular*": change in geographical distribution, spread and severity of the threat concerned and of the means of detection, if available.

This tool is supposed to function as a kind of *ad hoc* surveillance for the above health threats, and for this reason, it requires the mutual co-operation of Member States and the Commission via the channel of EWRS or the Health Security Committee. But it is not clear what will be the exact scope of shared data, what is the relation between the *ad hoc* monitoring and the EWRS, and, above all, whether *ad hoc* monitoring can involve exchange of personal data. That is why, it was concluded by the European Data Protection Supervisor that those problems raise questions regarding the protection of personal data.[31] The required implementing legislation which could perhaps provide answers to some of the questions has not yet been adopted by the Commission (see further section 4 below).

[29] Art. 8 para. 2 and Art. 10, para. 1, ECDC Regulation 851/2004; and Report on the implementation of Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No. 2119/98/EC (The 2015 Report) 9. See further: Sonia Kittelsen, "Conceptualizing Biorisk: Dread Risk and the Threat of Bioterrorism in Europe" (2009) 40 *Security Dialogue* 51.

[30] Art. 7 para. 1, Health Threats Decision.

[31] Conclusions, European Data Protection Supervisor Opinion on the proposal for a decision of the European Parliament and of the Council on serious cross-border threats to health, 28 March 2012, p.7, (EDPS Opinion 2012) <https://edps.europa.eu/sites/edp/files/publication/12-03-28_threats_health_en_0.pdf> (accessed 20 May 2017).

3. Individual Contact-tracing: Scope and Operation

The procedure of exchanging information between the responsible authorities in order to find and identify infected or potentially infected persons who were put in danger because of contact with, e.g. a pathogen or a chemical substance, is the next tool of public health control here examined.[32] Pursuant to the legal definition in Article 3(c), Health Threats Decision, contact tracing means:

"(…) *measures implemented in order to trace persons who have been exposed to a source of a serious cross-border threat to health, and who are in danger of developing or have developed a disease*."

A decision to trace contacts can follow the notification of Article 9 alert, but it can also be initiated earlier, at the national level, and then continued at the EU level through a co-ordinated action of Member States. The ECDC usually issues non-binding opinions on whether contact tracing should be applied for any specific disease and/or event in the course of its risk assessment, but the co-ordination of measures is decided at the Health Security Committee composed of national representatives.[33] Finally, it is always national CAs who, following the EDCD guidelines, ultimately decide, each according to its own procedures and national laws, whether contact tracing should be initiated in its jurisdiction with respect to a particular threat and carried out at national level of a given state. Normatively, it is national, administrative decision(s), although co-ordinated via EU level action.

As explained above, the exchange of data is to take place solely between the Member States affected by a health threat and via the EWRS selective module.[34] The type of individuals' data which are usually shared via EWRS under the contact tracing procedure include both personal data: e.g., contact details of the person, start of travel, means of transport, and other data related to the person's travel itinerary and places of stay, including, information on visited persons and destinations, and details of other persons potentially exposed to contamination; but also very often, sensitive health data, mainly information on alleged infection of sought individual(s) or on a possibility of developing an infection.[35]

[32] Art. 3f), and also, recitals 25-27 of the Preamble, Health Threats Decision.
[33] Art. 17, Health Threats Decision and Art. 4, Implementing Decision on Alerts. See also Stefan Elbe, *Security and Global Health* (Polity Press, 2010) 1-66.
[34] Art. 9 para. 3 i) and Art. 16 para. 2, Health Threats Decision.
[35] Cf. Old Commission Data Protection Guidelines, point 4 and Report from the Commission on the operation of the Early Warning and Response Systems (EWRS) of the Community Network for the epidemiological surveillance and control of communicable diseases during years 2004 and 2005 (The 2007 Report) (COM(2007) 121 final) 8.

The best way to explain the functioning of EU contact tracing is to cite some statistical examples from the Commission reports.[36] In 2006 there were 138 warnings and 223 comments of national CAs notified in EWRS; while in 2007, there were 105 warnings and 157 comments of national CAs respectively, nine of which triggered a need to co-ordinate response at the Union level and to those the comments related mostly (126/157). In the years 2013-2015, Member States authorities notified 168 warnings and posted 354 comments.
In a number of cases, the contact tracing procedure was initiated including the exchange of personal data across borders. For example, the 2007 Report describes a story of a rabies-infected dog, brought illegally into the EU, which had contacts with many people, including children, in the south of France. The application of contact tracing within EWRS allowed for sending rapid information and vaccination of affected individuals.[37] Another reported case concerned tracing back passengers of a flight from Thailand who have/might have encountered with a co-passenger smuggling into Europe in his hand-luggage two birds of prey, infected with the highly pathogenic avian influenza virus type A/H5N1, and intercepted at the Zaventem airport in Bruxelles. The next example of contact tracing occurred after several guests who stayed at the same hotel in Phuket (Thailand) were diagnosed with Legionnaires' disease, a serious lung infection. As a result, 284 tourists were identified and contacted with an information about the possible exposure and advised to seek medical care should they develop symptoms suggestive of Legionellosis.[38]
The above examples show visibly that the applied measures realised the goals of ensuring public and individual health. However, they also show that the application of contact tracing measures will always concern the exchange of personal data, and almost always, sharing of some kind of personal health data, usually without a preceding consent of individuals (because people are sought in the context of a health threat without being aware of it). In those cases, the EU system allows – within a prescribed legal framework – for the exchange of personal data, including sensitive, medical data, without a preceding consent of data subjects in the aim of protecting public health. This lawful limitation of the right to data protection is based on the legal basis in the general EU Data Protection Laws and on the safeguards included in the Health Threats Decision. Acting in obedience to those laws when personal data are exchanged in the EWRS is essential for the adequate protection of personal

[36] The 2007 Report 5-6; the 2009 Report 3; and the 2015 Report 9. See also Report on the Operation of the Early Warning and Response System of the Community Network for the Epidemiological Surveillance and Control of Communicable Diseases during 2002 and 2003 (The 2005 Report) (COM(2005) 104 final).
[37] See also Francisco Bombillar, "The Case of Pandemic Flu Vaccines: Some Lessons Learned" (2010) 1 *European Journal of Risk Regulation* 427.
[38] The 2007 Report 5 and the 2009 Report 6.

information under the EU regime of health threats. Before moving to the analysis of specific data protection safeguards in the Health Threats Decision, it is appropriate to investigate the legal basis for the exchange of personal (health) data in view of the general EU laws for safe data processing.

4. Legal Basis for an Exchange of Personal (Health) Data in the EWRS Pursuant to the EU Data Protection Laws

The general EU Data Protection Directive 95/46/EC applies to the processing of personal data by national authorities (e.g. within EWRS); and the general Regulation on Data Protection 2001/45 applies to the processing of personal data by the EU institutions (e.g. the Commission, ECDC).[39] The Directive will be repealed by the EU General Data Protection Regulation 2016/679 as of 25 May 2018.[40] These acts establish an EU-wide, horizontal system of data protection which is applicable to all policy fields, and providing legality conditions, general principles, obligations of data controllers, rights of data subjects, etc. which must always be obeyed by Member States (harmonisation of national laws) and the EU institutions respectively.[41] The laws give a specific enforcement framework to the right to personal data protection as provided for by Article 8(1) of the EU Charter of Fundamental Rights and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).[42] In light of the EU Data Protection Laws, the processing of personal data (contact tracing data) within the EWRS must always be justified on the basis of specific legal grounds. In this regard, Article 7 of Data Protection Directive (Article 6, GDPR), and the corresponding provisions of Article 5 of Regulation on Data Protection by the EU, set out the criteria for making data processing lawful and legitimate. Accordingly, an exchange of personal data in a contact tracing procedure can happen only if: (i) responsible authorities act to comply with

[39] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31; Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1.

[40] References to the repealed Directive will be construed as references to the Regulation, the Regulation on Data Protection 2001/45 will still apply to EU institutions, Art. 2, 94 and 99, Regulation (EU) 2016/679 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, "GDPR") [2016] OJ L 119/1. In the text, I provide references to both acts as necessary.

[41] See generally Orla Lynskey, *The foundations of EU data protection law* (Oxford University Press, 2015).

[42] See also Yvonne McDermott, "Conceptualising the right to data protection in an era of Big Data" (2017) January-June *Big Data & Society* 1; Bart Van der Sloot, "Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation" (2014) 4 *International Data Privacy Law* 307.

their obligations to prevent and combat serious cross-border health threats pursuant to the Health Threats Decisions ("*processing is necessary for compliance with a legal obligation to which the controller is subject*"); and (ii) the exchange is necessary to provide endangered persons with the appropriate care or treatment, with the aim of protecting the health of the concerned individuals and, ultimately, that of EU citizens at large ("*processing is necessary in order to protect the vital interests of the data subject*"); and (iii) the exchange is done to co-ordinate the response against health threats in the public interest ("*processing is necessary for the performance of a task carried out in the public interest*").[43] In other words, apart from a clear legal basis for an exchange (lawfulness), personal data may be processed in the EWRS only for specified, explicit and legitimate purposes and should not be further processed in a way incompatible with those purposes (the purpose limitation principle).[44]

Moreover, when processing of data within EWRS involves sensitive health data as well (and as explained above, it will mostly, or almost always be the case), processing must be additionally justified because a higher level of protection is accorded in the EU to the so-called sensitive data, including data regarding person's health.[45] That is why, EU law contains in principle a prohibition to process any health data which belong to the "special category of data" (Article 8(1), Data Protection Directive; Article 9(1), GDPR; and Article 10(1), Regulation on Data Protection respectively).[46] The exception to this general prohibition is possible in few situations, that is, when a data subject has given an explicit consent; when it is a vital interest of a data subject who is incapable of giving consent; and finally, when processing is required for "preventive medicine, medical diagnosis or healthcare and carried out by healthcare professional obliged to professional secrecy".[47]

Neither of those statutory exceptions from the Data Protection Directive refers explicitly to the situation of cross-border health threats, probably because when Directive was adopted in 1995 the Health Threats Decision did not exist. The new GDPR (repealing Data Protection Directive as of May 2018) introduces a specific exception in case of health threats (public interest). The exception applies when:

(…) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health (…), on the basis of Union or

[43] Art. 7(c, d, e), Directive 95/46, Art. 6(c, d, e), GDPR in connection with the provisions of Health Threats Decision. See Old Commission Data Protection Guidelines, point 4.
[44] Art. 6, para. 1(a-b), Data Protection Directive, Art. 4, para. 1(ab); and cf. Art. 5, para. 1(a-b), GDPR.
[45] See C-101/01 *Bodil Lindqvist* [2003] I-12971.
[46] See C-404/92 *P X v Commission* [1994] I-04737 and *Handbook on European data protection law*, supra, note 24, 42-45.
[47] Art. 8, para. 2(a)(c-d), and para. 3-4, Directive 95/46 which are in principle reflected in Art. 6(a), (d) and (e), Art. 7 and 9, GDPR.

Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.[48]

This development is very important for it makes the health threats regime more coherent with the EU Data Protection Laws, and reinforces the obligation both for the EU and Member States to provide for safeguards of rights of data subjects in that. Especially, when it can be very difficult to obtain explicit consents of data subjects. It is because of both objective conditions (e.g. data subjects are sought and they do not know they have contacted a source of a threat) and subjective circumstances (e.g. data subjects are incapable of expressing their consent). The very idea of EWRS functioning relies on the necessity of rapid reaction in situations of exceptional, cross-border health threats which may *per se* exclude any chance of seeking consent of data subjects. In any case, if it is feasible, authorities should seek to ensure that data subjects have given unambiguous consent for processing of their personal health details.[49]

Finally, the interpretation of Article 8 of the Charter by the EU Court of Justice ("CJEU") provides for an additional standard of control for the lawful limitation of the right to data protection in the context of health threats.[50] The case-law on processing of personal health data is scarce. However, the CJEU maintains, making often with reference to the case law of the European Court for Human Rights, that any transfer of health information by a public authority, may only be justified if: (i) it is "in accordance with the law", (ii) it pursues an objective which is exhaustively listed and (iii) it is "necessary" (proportional) to achieve that objective.[51] CJEU emphasises that "*In view of the extremely intimate and sensitive nature of medical data, the possibility of being able to transfer or communicate such information to a third party, even where that party is another European Union institution or body, without the consent of the person concerned, calls for particularly rigorous examination*".[52] Accordingly, a particular weight will be accorded by the Court to the proportionality assessment of a given action.[53] Any evaluation, however, will need to be contextualised in relation to a prescribed regime for health threats.

---

[48] Art. 9, para. 2(i), GDPR.
[49] See also *Handbook on European data protection law*, supra, note 24, 92-93.
[50] See also C-92/09 and C-93/09 *Volker and Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECR I-11063 and C-293/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.
[51] See F-46/09 *V v PE* [2011] ECLI:EU:F:2011:101, para. 112-113, C-404/92 *P X v Commission*, para. 18; and by analogy joined cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk* [2003] ECR I 4989, para. 73-75.
[52] F-46/09 *V v PE*, para. 123, referring to Eur. Court HR, Z v Finland, 1997-I, § 95. See also Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action" in Serge Gutwirth et al. (eds), *Reinventing Data Protection?* (Springer Science, 2009).
[53] See e.g. F-46/09 *V v PE*, paras. 121-150.

Consequently, in the present context, when a contact tracing measures is scrutinised, the exchange of personal data, especially of sensitive medical data, will be lawful if it is based on specific legal provisions and safeguards (here: Health Threats Decision and its implementing acts), it is undertaken by empowered authorities for the sole purpose of identification of individuals who have been exposed to a threat and to protect them (and others), and finally indispensable (necessary) for the co-ordination of a response against a health threat. The respect for the right to data protection will further depend on the guarantees embodied in the Health Threats Decision. Their analysis follows in the next section.

III. The Safeguards for Lawful Exchange of Personal Data in EWRS under the Health Threats Decision

The gradual development of statutory provisions and institutional solutions to protect personal data in the field of EU policy on health threats has been responsive to the establishment of increased number of electronic, Internet-based, communication tools between national CAs. The latter reacted to global risks of, e.g. diseases and bio-terrorism, fuelled by international mobility and discovery of new pathogens.[54] The adoption of special WHO rules to tackle international health emergencies (2005) was an additional, external factor which influenced the design of EU solutions.[55] So, the need to ensure populations' health resulting from the developing public health security agenda, prompted the employment of more technologically advanced means, which in turn required a better protection of data processing and personal privacy – it can be seen as a mutually reinforcing process.[56] The present EU system of data protection in case of public health measures results also from two widespread internal trends. The first one can be identified as a progressive modernisation of the legislative framework regarding the right to personal data protection.[57] The second one concerns the growth of EU competence and integration in the field of health with the respective results for institutional and policy choices.[58]

---

[54] See Gregory Koblentz, *Living weapons: biological warfare and international security* (Ithaca-London 2009); and e.g. ECDC, Rapid Risk Assessment – Zika virus disease epidemic (May 2016); EUobserver, Tuberculosis - an old plague comes back stronger (February 2013).

[55] See recitals 5-8 of the Preamble, Commission Decision 2009/547/EC of 10 July 2009 amending Decision 2000/57/EC on early warning and response system for the prevention and control of communicable diseases [2009] OJ L 181/57 (Old EWRS Decision).

[56] See generally Lawrence Gostin, *Global Health Law* (Harvard University Press, 2014).

[57] See Serge Gutwirth et al. (eds) *Reforming European data protection law* (Dordrecht, 2015).

[58] See Anniek de Ruijter, *A Silent Revolution: The Expansion of EU Power in the field of Human Health* (Ph.D. thesis, University of Amsterdam, 2015); Tamara Hervey, John McHale, *European Union Health Law: Themes and Implications* (Cambridge University Press, 2015).

This section examines the data protection safeguards in the Health Threats Decision, but it begins with the overview of initial guarantees established for the operation of the Old EWRS for infectious diseases. It does so for two reasons: first, to offer the historical background of the new system, second, to show the Reader the way the guarantees were developed.

1. Data Protection in the Old EWRS for Infectious Diseases – an Overview of Initial Guarantees

The initial regulation establishing the EU control system of infectious diseases and EWRS based on the Old Surveillance Decision and the Old EWRS Decision did not entail any specific provisions regarding protection of personal data. These matters were solely regulated by the provisions of the horizontal EU Data Protection Laws (of Data Protection Directive with obligations for national actors and Regulation on Data Protection for the EU institutions), but there was no reference to those laws in the health threats regime.[59]
Soon, as already mentioned in the introduction to this section, an appealing need to adopt more context-specific legal guarantees for the protection of personal and health data shared via EWRS emerged. The first important changes were introduced in 2004-2005.[60] In May 2005 a special communication channel was activated within EWRS to transmit messages related to data shared under the contact tracing. An SMS messaging function was also activated in order to transmit to the Commission users' the real time notification by SMS that an urgent message was posted on EWRS.
Second, the Old EWRS Decision was amended in 2009 especially to raise the standards applicable to data protection when contact tracing was applied.[61] A new Article 2a, which was inserted in the Decision, provided for a first legal definition of contact tracing, at that time, and for additional requirements of responsible authorities. That is, national CAs became statutorily obliged to use only "selective messaging functionality" when communicating personal data for contact tracing purposes. Second, sharing of data became permissible between the Member States affected by a disease only. Further, all the EU/national actors became explicitly bound to comply with the general EU Data Protection Laws while communicating and circulating personal data through EWRS.[62] Finally, Annex III was added to the Old EWRS Decisions containing for the first time the EU-level, indicative list of

[59] Now Art. 16, Health Threats Decision includes explicit references to the EU Data Protection Laws.
[60] The 2007 Report 7-8.
[61] Commission Decision 2009/547/EC of 10 July 2009 amending the Old EWRS Decisions 2000/57, supra, note 55.
[62] Art. 2a, para. 1-5, Old EWRS Decision 2000/57 as inserted by Art. 1, Decision 2009/547.

personal data which can be exchanges via EWRS under contact tracing. The list stipulated five categories of data which could be exchanged when seeking persons exposed to an infectious disease: personal information; travel specifications; contact information, including the names of visited places and persons; information on accompanying persons; and emergency contact details.[63]

Third, the Commission notified the EWRS to the European Data Protection Supervisor ("EDPS") for an „ex-post" check, in order to ensure that the tool respects an adequate level of data protection.[64] In his opinion, EDPS indicated several deficiencies in the analysed system, but eventually, he concluded that the EWRS is compatible with the general EU data protection framework provided that his recommendations are implemented.[65]

To remedy the enlisted defects, the Commission issued broad Data Protection Guidelines for EWRS users (2012).[66] The recommendation contained the explanation of principles for data protection in a given context, the clarification of duties assigned to EU/national actors ("data controllers"), their specific obligations, and the explanation of data subjects' rights with the necessary references to the EU Data Protection Laws. The Commission recommended that data controllers exchanging personal information in the contact tracing procedure should always assess its need on a case-by-case basis, following a scientific cost-benefit analysis in relation to the nature of the disease and advantages of its combating, and with a due respect to the proportionality of measures, considering whether data-sharing is "strictly necessary" for the purpose of applied measures.[67] The Old Guidelines also recommended, that national CAs ensured a technical design of data friendly environment, appropriate information to all data subjects, and an effective protection of their rights at the national level. Regarding the material scope of personal data which could be exchanged, the Commission advised a narrow interpretation of the indicative list from the Annex III to the Old EWRS Decision, stating that it "(…) *should not be seen as granting a blanket and unconditional authorisation to process these categories of data*". Moreover, in order to respect the proportionality principle, the Commission urged national CAs to apply an extreme precaution "*as regards processing of*

[63] See Annex III, Old EWRS Decision 2000/57 as amended by Decision 2009/547.
[64] See European Data Protection Supervisor, Prior checking opinion on the Early Warning Response System ("EWRS") notified by the European Commission on 18 February 2009 (case 2009-0137) (Brussels, 26 April 2010), http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2010/10-04-26_EWRS_EN.pdf (access 21 May 2017).
[65] EDPS, Prior checking opinion on the Early Warning Response System (26 April 2010) 7-17.
[66] The Old Commission Data Protection Guidelines 2012/73, n 26 above.
[67] Old Commission Data Protection Guidelines, point 6, pp. 38-39.

personal data other than those listed in that Annex, as disclosure is likely to be excessive and unreasonable."[68]

To sum up, as of 2012, the initial system of safeguards for personal data protection within the EWRS for infectious diseases was based on specific provisions of the Old Surveillance Decision, the Old EWRS Decision (as amended by the Decision 2009/257) and on the Old Commission Data Protection Guidelines. The acts were referenced to and consistent with the EU Data Protection Laws for national and EU authorities (Directive 95/46 and Regulation 2001/45). That system was fairly complete and normatively consistent to offer an adequate level of data protection on the condition that all the obligations and laws were respected by respective actors.

Now, the normative situation has changed. As a consequence of the reform of the EU regime on health threats, starting in 2013, the safeguards for data protection, in the context of their exchange within EWRS, are based on the new Health Threats Decision and its implementing legislation (so far incomplete), and as before, on the general EU Data Protection Laws.[69] The Decision absorbed in part previous guarantees resulting from the Old EWRS Decision, especially, regarding obligations for CAs and the guarantees built in technical structure of the EWRS platform. The only act of the initial system of data safeguards within the health policy which remains in force is the Old Commission Data Protection Guidelines. Notwithstanding its soft law character, it contains plenty of important explanations for national CAs and EU institutions as well as the suggestions for best practice in the implementation of personal data protection within EWRS. Yet, it was issued in the context of contagious diseases only, so it still ought to be updated and linked to the new Health Threats Decision.

Let us now turn to the new provisions.

2. Article 16 of the Health Threats Decision and the Current Personal Data Protection System

The new Health Threats Decision contains a specific Personal Data Protection Clause (Article 16 "Protection of personal data"). It was included in the Decision to provide for a set of specific safeguards ensuring the safe and lawful exchange of personal data in the

[68] Old Commission Data Protection Guidelines, point 6.4, p. 39.

[69] Health Threats Decision repealed the Old Surveillance Decision in 2013. The next two acts, the Old EWRS Decision as amended by Decision 2009/547, are now repealed by the Commission Implementing Decision on Alerts. See below.

application of the Decision, as implemented by Member States at national level and co-ordinated via EU actions.[70] The legal meaning of Article 16 can be explained as follows. The clause is a *lex specialis* to the general EU Data Protection Directive (soon: GDPR) and the Regulation on Data Protection by the EU institutions. The purpose of this provision is to implement the EU general data protection principles in the field of public health (relating to purpose limitation, data quality and retention, confidentiality and security).[71] That is why, Article 16 imposes some stricter requirements both on national and EU authorities when they apply the Health Threats Decision, especially, when they share personal data in the EWRS under contact tracing procedure. Article 16 contains several context-specific (public health), particular obligations for national CAs (e.g. to use solely the selective messaging functionality of EWRS to communicate personal data) and implementing powers for the Commission (e.g. to issue guidelines ensuring that the day-by-day operation of the EWRS complies with the general EU Data Protection Laws – to be – "the New Commission Data Protection Guidelines").[72] Moreover, it designates the particular responsibilities of data controllers under the Health Threats Decision to ensure their proper enforcement. That is, national CAs are regarded as data controllers in relation to responsibilities to notify and rectify personal data through the EWRS (information and rectification rights of data subjects); and the Commission acts as data controller concerning storage of personal data.[73] It is a consequence of the fact that EWRS is an example of joint controllership, where the responsibility for ensuring safe processing of data is allocated, at different levels, between the Commission and the Member States.[74] Finally, Article 16 also mandates several operative and technical functions of EWRS required for data protection, for example: accessibility to personal data exchanged in the system is restricted to affected Member States only, selective messaging function is mandatory for personal data sharing, and duration of processing is limited. For example, EWRS CAs receive login and password from the Commission together with an authorisation for a full access to both channels and the two functions of the EWRS: reading and commenting messages. Since August 2015, the access to EWRS has been granted through the special authentication system of the Commission (ECAS) and through personalised email addresses and passwords, although some Member States expressed preference for access

[70] Recital 27 of the Preamble, Decisions 1082/2013.
[71] See e.g. Art. 6(1)(b-e), 16, 17, Directive 95/46 and 4(1)(b-e), 21, 22 Regulation 2001/45.
[72] Art. 16, para. 3 and 9(a), Health Threats Decision.
[73] Art. 16, para. 7 and 8, Health Threats Decision.
[74] Art. 16, para. 1, Health Threats Decision. See also: the Old Commission Data Protection Guidelines, points 7 and 9 and EDPS Opinion of 26 April 2010.

through "generic mailboxes".[75] The system of safeguards for lawful personal data sharing within EWRS (as of 2017) is presented and described in detail in Table 1.

It should further be emphasised that, in order to warrant lawful and legitimate data processing, the Health Threats Decision refers in its content more explicitly to the purpose of data exchange and the proportionality of applicable measures. In light of its provisions, national CAs are allowed to communicate solely those personal data which are "*necessary for the purpose of contact tracing*". In other words, the clear purpose of personal data exchange is established in the Decision in order to provide a yardstick for the assessment of respective measures. This sole aim is identification of persons who were exposed to a serious health threat and risk developing of a disease or have it already developed. Moreover, communication of personal data via EWRS must be "*useful*" for co-ordination of a response to a serious cross-border health threat. Accordingly, the proportionality of measures will be assessed against this condition, that is, whether sharing of personal data was suitable and necessary to respond to a given threat. It would also often require a reference to scientific evidence based on a specific risk assessment (performed by the ECDC and/or national CAs). Further, in case of finding that exchange of personal information was unnecessary for contract-tracing measures, CA concerned must immediately inform other involved authorities.[76]

Further, for matters not regulated in Article 16 Personal Data Protection Clause, responsible actors are obviously obliged to apply the provisions of the general EU Data Protection Laws to ensure safe data processing. Article 16 provides for an explicit reference to that framework.[77] As already explained above, national CAs must respect the Data Protection Directive (and as of 18 May 2018 GDPR) and EU institutions, the respective Regulation on Data Protection.[78] The provisions of those acts will apply to the issues not tackled in Article 16, for example, legal definitions relevant for data protection (e.g., "data controller", "processing"), provisions establishing information and access rights of data subjects, and obligations to notify and rectify incorrect data in the EWRS.[79]

[75] Art. 15 para. 1, Health Threats Decision. See: the 2015 Report, p. 8.
[76] Art. 16 para. 6, Art. 9.3 and Art. 9.3(i).
[77] Art. 16, para. 1, Health Threats Decision; cf. the Old Commission Data Protection Guidelines, point 4.
[78] See e.g. Art. 10-11, Directive 95/46 (GDPR) and Art. 11-12, Regulation 2001/45.
[79] Cf. the Old Commission Data Protection Guidelines, points 8-9 and 11.

SAFEGUARDS FOR LAWFUL PERSONAL DATA SHARING WITHIN EWRS (AS OF 2017)		
TYPE	**DESCRIPTION**	**EU LEGAL BASIS**
Limited accessibility to personal data exchanged	▪ EWRS is accessible only to authorised users: national CAs (focal points as designated by Member States), the Commission and ECDC ▪ access is protected via secured and personalised user account and password ▪ a warning is visibly displayed in the EWRS messages overview page, informing users that the general messaging channel is not designed for accommodating contact tracing and other personal data	Article 15.1(b) and Article 9.3(i), Health Threats Decision; Article 1.1 Implementing Decision on Alerts the Old Commission Data Protection Guidelines, point 7
Selective messaging (obligations for competent authorities)	▪ personal data must be communicated via "selective messaging functionality" built in EWRS ▪ personal data may be communicated to national CAs involved in contact tracing measures only ▪ the other EWRS users, the Commission and the ECDC are automatically excluded from access to personal data exchanged through the selective messaging channel (unless access is needed for a co-ordination of action);	Article 16.2-3, Health Threats Decision; the Old Commission Data Protection Guidelines, point 7
Day-to-day correction of personal data & limited duration of processing	▪ EWRS has a built-in, on-line feature allowing for rectification and deletion of selective messages containing personal data which is inaccurate, not up-to-date, no longer needed, or incompatible with data protection laws; ▪ there is a specific mechanism in the selective messaging channel allowing CAs involved to communicate and cooperate on requests of data subjects ▪ a built-in, on-line feature of EWRS automatically erases messages containing personal data from the selective message functionality 12 months after the date of their posting;	Article 16.3-4 and 6, Health Threats Decision; the Old Commission Data Protection Guidelines, point 7 and 9 Article 16.5, Health Threats Decision
Designation of responsibilities of data controllers	▪ controllers' duties are shared between MS (notification, and rectification), and the Commission (storage) to ensure their proper enforcement under the joint controllership of the Commission and national CAs (ECDC acts as "processor"); ▪ there is duty for a national CA to immediately inform other CAs concerned that data processing was in breach of the EU Data Protection Laws (because it was unnecessary).	Article 16.1 and 16.5-8, Health Threats Decision; the Old Commission Data Protection Guidelines, point 8-9; Article 20, para. 4, ECDC Regulation 851/2004.

Table 1. Safeguards for lawful exchange of personal data in EWRS (source: own analysis).

In sum, and as can be seen in the Table 1 above, the system of data protection safeguards established under the Health Threats Decision provides a broad set of important guarantees to ensure safe processing of personal data.

It also appears that they function well in practice. The Commission Report of 2015 on the implementation of the new Decision contains the optimistic information. First, the system has been technically adjusted to the new material scope of the Decision – "*the existing IT tool of the EWRS was expanded to include threats of biological, chemical, environmental and unknown origin*". The new version of this IT tool was put in place in February 2015.[80] Second, during the 2014 Ebola epidemics in Africa, the selective messaging functionality of EWRS proved to be crucial for the transmission of personal data to support the medical evacuation of patients from the affected countries into the EU.[81]

[80] The 2015 Report 7.
[81] The 2015 Report 3.

So far so good. Operationally, the EWRS is said to be adjusted to the provisions of the Health Threats Decision. However, from a normative point of view, including the law enforcement, there are still many issues which raise doubts. The next section proceeds to their critical appraisal.

IV. The Problems of the Effective Personal Data Protection – a Critical Appraisal

When one carefully scrutinises all the provisions pertinent to the prevention of health threats, and the EU/national websites relevant to this policy, it becomes apparent that there are several shortcomings of the system which can affect the enforcement of personal data protection. Especially, one can imagine that when future use of contact tracing measures and EWRS is necessary on a broad scale, the adequacy of legal protection of data subjects and their rights can be easily affected by those shortcomings.

1. The Incompleteness of the Regime

It has been already repeated several times throughout the piece, that as a result of the regulatory reform, the new Health Threats Decision has the broader material scope. The today's regime covers biological (diseases), environmental, chemical, and other health threats, when the 1990s' regime regarded communicable diseases only.[82] It is a consequence of the EU "integrated approach" to health and security. Accordingly, the new Decision requires new implementing acts (old implementing legislation is now repealed), but as of September 2017, the Commission has not yet issued relevant implementing provisions (the Health Threats Decision entered into force in 2013).[83]

First, neither Health Threats Decision nor Implementing Decision on Alerts (which repealed the old EWRS Decision) specify an indicative list of personal data which could be lawfully shared for contact tracing purposes. The Old EWRS Decision contained the Annex III where an indicative list was provided as an important yardstick for the application of the principles of lawful data processing: the purpose limitation and the proportionality evaluation. The relevant guidelines should be adopted by the Commission (Article 16, para. 9(a), Health Threats Decision). Second, the Commission should also issue new guidelines ensuring that

[82] Cf. the Old Surveillance Decision 1–7; the 2015 Report 8, point 2.5.
[83] A de facto transitory period has been lasting for too long now – since 2013 one implementing act has been issued: Implementing Decision on Alerts of 2017, *supra*, note 21.

the operation of EWRS is compatible with the general EU Data Protection Laws (as required by Article 16, para. 9(a)). Since 2013 when the new Decision entered into force, the system has been relying on the Old Commission Data Protection Guidelines of 2012 which were issued for the EWRS for infectious diseases. Third, there are no updated or adjusted implementing or delegated measures to Article 6, para. 5 of Health Threats Decision (the list and case definitions for communicable diseases and related health issues); Article 7 para. 3 (case definitions to be used for *ad hoc* monitoring); Article 8 para. 2 (procedures for the information exchange and operation of EWRS), and Article 11 para. 5 (procedures for uniform implementation of CAs' co-ordination).

The existing gaps in the regulatory system which result from the lack of implementing legislation can easily affect the clarity of data protection safeguards and their accurate enforcement. To give several examples: the current EU legislation does not provide for an indicative list of personal data to be exchanged for contact tracing purposes. The differences between national systems in that respect can affect the system of data protection because it is possible that divergent data are collected or required by different national CAs. In effect, it is possible that in various Member States different data are collected in the context of different catastrophic situations, involved diseases and/or other health threats. Some Member States may collect and exchange personal data which in light of other national systems will be illegitimate and/or unnecessary. To put simple, it is contestable whether it is a name, address, and phone number which are necessary for identification; or just a name and date of birth? What about the information on sex and nationality?[84]

Without a harmonised, indicative list stating which personal data can be lawfully exchanged, it can be difficult to agree what data constitute "a minimum threshold" for individuals' identification under contact tracing measures (to remind: only those data of an individual can be communicated which are necessary for identification of persons who have been exposed to a threat). Previously an indicative list of data which could be exchanged provided a useful framework of reference. The current lack of an EU-wide standard which personal data can be exchanged for the purpose of contact tracing creates a deficiency in the regime regarding the lawfulness and the legitimate purpose of data processing.

Further, the current legal definition of contact tracing is relatively general. Already in 2010 and in 2012, the EDPS recommended that a more structured format for the exchange of

[84] See e.g. the controversy between the Polish Data Protection Authority and Publish Health Authority regarding whether the exchange of information on "nationality of data subject" is necessary for contact tracing purposes, http://www2.mz.gov.pl/wwwfiles/ma_struktura/docs/chorobotworz_20121206_odp_04.pdf (accessed 20 May 2017).

contact tracing information should be provided, as well as a clearer definition of contact tracing, indicating its purposes and scope, methods for determination of the persons to be sought, and sources that can be used to obtain contact details, which might be all different for communicable diseases and other health threats.[85]

Moreover, some provisions of the old regime have disappeared. Before the adoption of the Health Threats Decision, the Annex to Old EWRS Decision regulated the criteria obliging to notify an alert within EWRS (for infectious diseases). They guided CAs when to institute an alert and provided for the 3-degree diversification of alerts. It remains unclear whether those issues would be regulated in implementing acts or not at all.

Next, at present, the relationship between *ad hoc* monitoring and the EWRS is not clear, especially, with regard to the specification of types of data which can be processed through the former. The provisions of the Health Threats Decision are not equivocal on this issue and it is not known what measures will be applied to minimise/exclude the chance of processing of personal data (e.g. through appropriate anonymization techniques and/or restriction of the processing to aggregate data).[86] Again, it would be helpful to address all the above matters, at least, in the legislation based on Health Threats Decision (which foresees appropriate powers to adopt implementing acts).

Finally, the criteria guiding the assessment of proportionality of contact tracing measures should be included in the implementing legislation.[87] They could address significance of risk assessment and scientific expert evidence mandating contact tracing, the relation between national and ECDC/WHO scientific evaluation, if diverse, and case-by-case evaluation of health threats.

To sum up, the first considerable, effect of the lack of adoption of implementing act to the Health Threats Decision (i.e. incomplete regulatory framework) results in ambiguity of the scope of powers and obligations of EU/national CAs ("data controllers"). The second, resulting consequence can be an inaccurate application of data protection safeguards. This, in turn, can lead to a contestation of lawfulness, legitimacy and proportionality of an exchange of personal data in the ERWS and the contact tracing procedure.

[85] EDPS Prior checking opinion on the Early Warning Response System (26 April 2010) 4-5 and 16; EDPS Opinion (28 March 2012) 7.
[86] Ibid.
[87] EDPS Opinion (28 March 2012) 7.

2. Insufficient Coherence of the Regime

The next shortcoming of the health threats regime which can affect the level of personal data protection is its insufficient normative coherence with other EU policies. It will be illustrated through the following examples.

The overall aim of EWRS operating under the Health Threats Decision is to complement the existing information security systems at the EU level in order to avoid duplication of information-sharing procedures.[88] Accordingly, the Decision foresees a progressive linking of all the EU, Internet-based alert tools with EWRS in the aim of streamlined communication of various health threats. The new Article 3 of the Implementing Decision on Alerts obliges the Commission to indicate through EWRS the lead system for the information exchange when a serious cross-border threat to health is communicated through more than one Union alert system. Yet, other systems (e.g. Rapid Alert System for Food and Feed, RASFF; Rapid Alert System for Dangerous Non-Food Products, RAPEX) do not have specific safeguards for the exchange of personal data. Will the lawfulness and legitimacy of processing of personal data be safeguarded in this context? The problematic character of those provisions is in part a consequence of an integrated approach to health and security in the EU (because before EWRS applied to infectious diseases only and there was no interest of linking it to other electronic systems).[89] It is also not clear how the guarantees for the adequate personal data protection (which are integral to the electronic platform of EWRS) will be implemented if CAs decide that they will communicate within the Health Security Committee in writing.[90]

It is also feared here that the transition between the system of the EU Data Protection Directive and its successor, the system of GDPR can lead to incoherence between the Health Threats Decision and the respective national laws – which will need to be adjusted to the new GDPR. Until 2017, the Data Protection Directive established the total harmonisation in the field of data protection,[91] but nevertheless, Member States were entitled to some exceptions, including those relating to stricter requirements in national laws for data protection in the EWRS.[92] The Regulation will substitute those national laws which had been earlier implementing the Data Protection Directive, but also require new, revised national laws. The final shape and content of national laws is impossible to predict, but there may well be gaps

[88] Art. 3 and Annex listing EU level alert systems, Implementing Decision on Alerts.
[89] See also Stefan Brem, Stéphane Dubois, "Different perceptions, similar reactions: Biopreparedness in the European Union", supra note 15.
[90] See Art. 4, Implementing Decision on Alerts.
[91] C-101/01 *Bodil Lindqvist*, para. 96.
[92] The Old Commission Data Protection Guidelines, point 4.

regarding the consistency between national laws allowing for the practical operation GDPR and the provisions of the Health Threats Decision applicable to exchange of personal data.

3. Insufficient Transparency for an Individual Citizen

Finally, the EU regime for combating health threats suffers from an insufficient degree of transparency for individual citizens. It concerns both ordinary citizens and persons affected by data processing.

To begin with, there is no satisfactory or simply none information on the Commission's website regarding the current EU regime for health threats, conditions for exchange of personal data in the context of EWRS and contact tracing measures. The DG SANTE webpage is divided into two folders: security and health threats; and control of communicable diseases, but the information provided is incoherent and outdated.[93] Various pages of the Commission's website list regulatory acts which are no longer in force.[94] The webpage of ECDC does not provide information on the respective issues either. All the sites are available in English mainly and it is not quite clear how data subjects are informed of the processing of their personal data. For example, there is no information regarding the exercise of access rights of data subjects (including rectification, erasure and blocking), the enforcement of rights against national CAs and their different jurisdictions, or at least, name(s) of a contact person in case of need.

Insufficient transparency is problematic because personal data processing in the contact tracing procedure happens between two or more Member States where different CAs collected and exchange personal data. It might even not be a country of origin of a given person. Supposedly, each person receives the information about contact-tracing measures and their consequences from national authorities, but what happens if the information is incomplete and/or a person does not understand it (language problem) and/or there is a mistake in the data content? Will this be clear to a person to whom his/her concerns should be addressed? Will this be clear which his/her personal data have been exchanged, and where they can be accessed/corrected, etc.? And what happens if links provided in e-messages do not function properly?

---

[93] Based on own research, see http://ec.europa.eu/health/preparedness_response/policy/decision/index_en.htm and http://ec.europa.eu/health/communicable_diseases/early_warning/comm_legislation_en.htm (access 23 September 2017).

[94] Even the Eur-lex data base contains a mistake that the Old EWRS Decision (2000/57/EC) is still in force, and the link provided from the page of Implementing Decision on Alerts, which repealed that act, directs us to the Directive 2000/57 on pesticides residue limits (access 23 September 2017).

It is difficult to provide definite answers to those questions. The lack of answers contradicts the Old Commission Data Protection Guidelines stating that a clear and comprehensive privacy statement will be available on the webpage dedicated to the EWRS.[95] It further ignores the recommendation of EDPS.[96] It also contrasts heavily with the Commission's original declarations that the reforming process of the previous regulatory framework (for infectious diseases) would lead to the simplification of existing legislation and the improvement of transparency.[97]

PROBLEMS OF ADEQUATE PERSONAL DATA PROTECTION WITHIN EWRS (AS OF 2017)	
Scope of data which can be legally processed	▪ an indicative list of the personal data that may be exchanged for the purpose of the co-ordination of contact tracing measures is lacking as the Commission has not yet issued a relevant Recommendation pursuant to Article 16, par 9(b), Health Threats Decision; ▪ the Implementing Decision on Alerts does not contain any respective provisions.
Doubts on law enforcement of data subjects' rights, e.g. access and information	▪ less effective application of EWRS safeguards in view of lacking of required implementing soft law to Article 9(a-b), Health Threats Decision (the old EWRS Decision was repealed); ▪ unclear if and to what extent EWRS safeguards apply in case of Article 7 *ad hoc* monitoring ▪ unclear how EWRS safeguards will apply after linking EWRS with other EU Alert and Information Systems ▪ insufficient transparency of the relevant websites and insufficient transparency safeguards

Table 2. Problems of adequate personal data protection within EWRS (source: own analysis).

To conclude the overall appraisal, it can be said, that the revision of the EU-wide regime for health threats to follow the "integrated approach" has not (yet?) introduced a comprehensive system to warrant personal data protection completely. The problems of an adequate personal data protection in the process of data exchange within EWRS are summarised in the Table 2. It is true that the Health Threat Decision and its implementing act establish the framework to ensure that processes of data exchange within EWRS are lawful, but a number of actions are clearly needed to address the above-described incompleteness, insufficient coherence and transparency of the EU regime for prevention of health threats. A basis step to begin with would be to adopt necessary legislative solutions, however, it may not be that easy because of a complexity of the new regime based on the "all-hazards approach". This is another reason why the health threats regime suffers from the above shortcomings: because it simply takes a very long time to adopt measures (of all kinds) which concern those intricate "all-hazards security" issues.

[95] The Old Commission Data Protection Guidelines, point 8; cf. https://ewrs.ecdc.europa.eu/ (accessed 30 September 2017).
[96] EDPS, Prior checking opinion on the Early Warning Response System (26 April 2010) 16.
[97] Commission staff working paper Impact Assessment Accompanying the document Decision of the European Parliament and of the Council on serious cross-border threats to health SEC (2011)1519 final, p. 48.

V. Conclusions: What Perspectives for Data Protection under EU Regime for Health Threats?

The detailed analysis in the preceding sections allows for the conclusion that the present EU policy on serious, cross-border health threats appears to prioritise "the integrated approach" to health and security over a complete and coherent system of provisions guaranteeing an adequate level of personal data protection. The shortcomings of the regime (the incompleteness, the insufficient coherence and transparency), which can often be linked to that approach, can affect the enforcement of the broad set of guarantees for the lawful data processing within EWRS, as established by the Health Threats Decision. If the claimed defects in the EU system are not remedied, the reform of the EU policy for health threats undertaken in the name of "all-hazards security" may lead to questioning of the rationale for the reform which involves big costs of adaptation to a broadened scope of application and is undertaken at the expense of adequate protection of personal data. It will further confirm that an increased security agenda for public health policy brings risk to the effective protection of individual rights.[98]

The case of Mr Speaker which was introduced at the beginning of this piece is exemplary in this respect. Ultimately, the authorities did not prove that he was dangerous to public health and the mistakes had been revealed regarding the scientific risk assessment (he was first diagnosed with XDR-TB, and then re-diagnosed with less dangerous MDR-TB). Yet, after his transatlantic tracing, all his personal and health data became world-famous and he was portrayed by political actors as a threat to public health security. It caused his stigmatisation, hysterical press reactions, and unnecessary public fear.[99]

This case also prompts the observation that a regulatory system which (lawfully) limits the individual right to personal data protection in the name of public health, but suffers from any inconsistence and incompleteness, can be even more vulnerable to infringements and misuse. It can be more easily exposed to politicisation of risk assessments and achievement of sole political gains by powerful actors should health threats arise.[100] It is also susceptible to the implementation of the politics of fear and further securitisation of public health in the form of

[98] See Therese Murphy and Noel Whitty, "Is Human Rights Prepared? Risk, Rights and Public Health Emergencies" (2009) 17 *Medical Law Review* 219.

[99] Wendy Parmet, "Dangerous Perspectives. The Perils of Individualizing Public Health Problems" (2009) 30 *Journal of Legal Medicine* 1.

[100] See also Kaci Hickox, "Caught Between Civil Liberties and Public Safety Fears: Personal Reflections from a Healthcare Provider Treating Ebola" (2015) XI *JHBL* 9.

unfounded limitation of data protection.[101] It also makes the scrutiny of legitimacy and proportionality of the exercise of powers of public health authorities and their administrative actions more difficult.

That is why, a comprehensive and enforceable system of safeguards for personal data protection is an absolutely basic standard which must be applied to ensure that lawful limitations are respected, that any infringements are minimalised, and any prohibited interference can be challenged against responsible authorities. The careful attention of policy-makers and the research community should be paid to these perspectives for personal data protection in the application of the EU regime for health threats.

[101] Cf. Wendy Mariner, "Medicine and Public Health: Crossing Legal Boundaries" (2007) 10 *Journal of Health Care Law & Policy* 121.