DATA PROTECTION IMPACT ASSESSMENT FOR REDCAP AND GO.DATA FOR DATA ANALYSIS PURPOSES

I. Introduction

The DPIA is a risk assessment that gauges the risk to the privacy of the data subjects by evaluating how personal data collected through two new tools, REDCap and Go.Data, are processed, stored, and accessed for the purpose of epidemiological prevention and control. It is an update of the previous DPIA performed for the outbreak investigation tool 'Voozanoo' which identifies potential vulnerabilities and assesses the safeguards to protect the data subjects' rights and freedoms.

Go.Data is an outbreak investigation tool that supports collection of data from contact tracing activities for epidemiological analysis purposes, whereas REDCap is a secure web platform for building and managing online databases and surveys that may be used by ECDC to is to facilitate data collection and analysis during disease outbreaks, facilitate epidemiological analyses and support assessment of preparedness for, response to and/or surveillance of communicable diseases.

The data subjects in this processing operation are **cases** (i.e. persons diagnosed with an infectious disease) and their **contacts** (i.e. persons who have been exposed to someone diagnosed with a disease).

II. Description of the envisaged processing operations and the purpose of the processing

a) Data flow diagram of the process

What is collected?

Case-based data may be collected and processed using a questionnaire created using REDCap, while data related to contacts are collected and processed via Go.Data. Only pseudonymized data are collected across both software platforms. Identifying attributes such as names, addresses, dates of birth, national insurance or national identification numbers will not be collected. Pseudonymized data might comprise demographic, clinical, epidemiological information (e.g. age, gender, country of residence), including information on exposure (e.g. food exposure, hotel stay, vaccination status), case identification numbers provided by the contributors and laboratory results.

ECDC does not have the information/key to re-identify data subjects in REDCap or Go.Data. Therefore, a confidentiality level similar to that observed for EpiPulse Cases data will apply.

From where/whom?

Access to REDCap and Go.Data is restricted to ECDC staff and nominated EU and EEA Member States users that provide the data or manage a project. Project coordinators and contributors of both tools shall ensure that only participants within the EU/EEA are nominated/invited.

What do we do with it?

ECDC does not use the data, unless a ECDC staff member initiates and/or manages a questionnaire on REDCap or an outbreak on Go.Data; in such situations, this person can export the data of that specific questionnaire/outbreak

for epidemiological analysis and reporting. Exported data must remain in the work IT environment though. Data are used by ECDC and Member States to strengthen and enhance technical support to or readiness activities; outbreak risk assessments; field investigations and response, including response research.

Go.Data and REDCap are complementary outbreak investigation tools, however there will not be automatic transfer of data from one tool to the other. No personal data is fed in from other systems.

Where do we keep it?

REDCap is fully hosted in ECDC's Microsoft Azure tenant (secured cloud-based servers located in the EU/EEA area with restricted access). Go.Data is currently installed as a standalone application in a virtual environment on-premises in ECDC's data center but may be migrated to ECDC's Microsoft Azure tenant in the future. Data collected through Go.Data are held on ECDC's Microsoft Azure tenant. Such processing is subject to the ECDC Information Security Policy and standard ICT security measures (ECDC/IP/63)

Who do we give it to?

User access management (i.e. who gets access to the server and the data within) for both REDCap and Go.Data is configured so that access is controlled and limited to nominated users on a project-specific basis. Nominated users can be national experts, public health or health care staff from EU/EEA countries, ECDC staff and representatives of other European authorities and international organisations.

Both the coordinators (ECDC staff or Member State National Focal Points) and the contributors (e.g. persons in community institutions and bodies, laboratories, academic and/or public health organisations) can input data and export the results of specific REDCap questionnaires or Go.Data outbreaks. Contributors may only access, enter and export their own data. Data that are not already made public shall be considered as confidential by users of the tools. No disclosure of confidential data to third parties is permitted unless ECDC or the relevant Competent Body requests that the data be made public in order to protect public health or if otherwise provided for by applicable legislation.

b) Detailed description of the purpose(s) of the processing:

The purpose of this processing operation is to analyse personal data for epidemiological prevention and control purposes, such as for example:

1. investigations of subnational, national or multi-country outbreaks,
2. epidemiological analyses in general, and
3. assessments of preparedness for, response to and/or surveillance of communicable diseases.

Go.Data supports this processing operation through data collection, contact tracing, contact follow- up, and visualisation of chains of transmission for epidemiological prevention and control purposes.

The use of these tools thereby enables ECDC to detect and monitor outbreaks of communicable diseases and to identify and assess emerging health threats. These tools may support the investigation of any type of infectious disease outbreak (e.g. food-borne disease outbreaks, mpox, outbreaks of Legionnaires' Disease and cross-border outbreaks of multidrug-resistant TB). They provide the possibility to build project-specific questionnaires (REDCap) or outbreaks (Go.Data) to collect and analyse data for descriptive and analytical studies and to adjust different roles and access levels to users. Thus, they can support a variety of epidemiological analyses and assessments of prevention, preparedness and response plans. Both tools are maintained and supported in-house by ECDC staff.

c) Description of the supporting infrastructure

REDCap is fully hosted in ECDC's Microsoft Azure tenant (secured cloud-based servers located in the EU/EEA area with restricted access). Go.Data is currently installed as a standalone application in a virtual environment on-premises in ECDC's data center, but may be migrated to ECDC's Microsoft Azure tenant in the future. Data collected through Go.Data and REDCap are held on ECDC's Microsoft Azure tenant. Such processing is subject to

the ECDC Information Security Policy and standard ICT security measures (ECDC/IP/63)

III. Assessment of the necessity and proportionality of the processing operations in relation to the purposes

Legal basis:

The legal bases of this processing operation are Articles 3 (1) and 3 (2) (a) and (b) ('Mission and tasks of the Centre'), Article 10 ('Identification of emerging health threats'), Article 5b (2) (a) ('review of national preparedness plans'), Article 11 ('Collection and analysis of data') of Regulation (EC) No 851/2004 as well as Article 8 (1) ('assessment of prevention, preparedness and response planning'), Article 13 (2) (b) ('detection and monitoring of cross-border communicable disease outbreaks with regard to source, time, population and place') and Article 18 (2) of Regulation (EU) 2022/2371, ('ECDC to use contact tracing technologies for the purpose of combatting serious cross-border threats to health').

Necessity:

Outbreak investigations and surveys for epidemiological analyses cannot be carried out with anonymised data. Data providers must be able to check and validate individual cases of communicable diseases and contacts to document compliance with scientific methodology, thereby safeguarding the scientific accuracy and integrity of the outbreak investigations or epidemiological analyses, respectively. It is thus strictly necessary to process personal data for these purposes.

Experience from the COVID-19 pandemic shows that processing case-based and contact-tracing data at large scale in a manual manner, is time-consuming, inefficient and prone to errors.[1] Therefore, a digital solution is needed to support this processing operation.

Many alternative tools were considered for this processing operation. It was concluded that REDCap and Go.Data were the most appropriate tools available to collect the information needed to fulfill this task in ECDC's mandate while remaining in full compliance with data protection regulations.[2]

The processing of personal data of cases and contacts is thus necessary to attain the purpose.

Proportionality:

Benefits of the processing operation include: (i) Collection of disease surveillance and contact tracing data relating to outbreaks; (ii) Assisting the identification of appropriate response action(s) required, and (iii) Supporting EU and Member States in their disease surveillance and response activities.

The risks to the fundamental rights of data subjects arising from this processing operation include a risk of disclosure of the personal data, which would breach the fundamental rights to personal data and privacy of the persons affected. However, all personal data have been pseudonymized. In case of a personal data breach, the data subjects cannot be identified. Thus, their right to privacy is safeguarded. Furthermore, standard ICT data protection measures have been implemented to secure the confidentiality, integrity and availability of the data. ECDC ensures that personal data are retained only for as long as necessary. Data will be removed from the application after one year following the completion of the project, and thereafter they will be deleted or anonymised. Only the minimum amount of data required to satisfy ECDC's mandate will be collected. Countries

[1] European Commission: European Health and Digital Executive Agency, Cesuroglu, T., Baron, R., van der Meer, A., van der Steen, S. et al., Feasibility study on digital technology for cross-border contact tracing – Final report – Version 2.2, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2925/21434, page 10.

[2] See Feasibility Assessment Report and implementation roadmap on Prevention, preparedness and response planning and reporting module

can also develop their own REDCap questionnaires or Go.Data outbreaks to limit the level of data collected even further. Data subjects are fully informed of the data processing operation undertaken.

With this said, the public health benefits outweigh the risks to the rights and freedoms of the data subjects.

IV. Assessment of the risks to the rights and freedoms of the data subjects and mitigating measures

Risk	Description and mitigating measures
IT Security risks	Threat events/vulnerabilities include: - External attack – hackers may target the public REDCap and Go.Data web services (URLs) - Internal or external misuse and abuse or theft of personal data - Unintended access to personal data processed by Go.Data or REDCap or any other ECDC ICT tool. These risks are mitigated by countermeasures including: - Pseudonymisation of all personal data processed required - Access to Go.Data and REDCap is controlled and limited to nominated users - User access management to REDCap is configured via ECDC's IAM solution. For Go.Data, access is configured manually. - Users are required to sign the Terms of Service (ToS) before being given access to both tools. - Strong username and password policies are in place and clearly described in the user ToS. - Both Go.Data and REDCap are part of ECDC standard operation and technical security controls - Automated daily backup service of the application databases are in place - Setup whitelisting of Member States (IPs) who can access the web service (URL) - Brute force protection and email 2fa are set up for the Go.Data application, which is. , isolated on the network with limited access between networks (e.g. port 443 for HTTPS only) - Apply application of the rules and procedures on storage and data sharing set out in IP 144 and IP 152 to Go.Data data by analogy - Establish a workflow to monitor staff and personnel turnover in order to

	timely revoke access in the medium-term - Risk level: limited
Transparency and exercise of data subjects' rights	Terms of Service for ECDC's installations of REDCap and Go.Data respectively have been drafted to cover the use of the tools and related data protection aspects. **All users** are required to sign the relevant Terms of Service and **acknowledge that they have been informed** about their rights and obligations before being given access to either tool. The Privacy Statement for the processing operation 'Data analysis for epidemiological prevention and control' and this DPIA will be published on ECDC's webpage to inform cases and contacts about the processing of their personal data. Despite its best efforts, ECDC cannot ensure that all data subjects (namely cases and contacts) will receive and take note of this information. Risk level: limited
Processes and legal framework	There is no specific procedure or instructional document governing outbreak investigations, contact tracing and preparedness evaluations yet. However, the instructional documents governing general surveillance and the analysis of case-based data for epidemiological purposes (e.g. TESSy policy) apply by analogy. All internal and external users of REDCap and Go.Data must accept ECDC's Terms of Service. These Terms of Service set out the responsibilities of users and impose on them technical and organisational measures that safeguard the protection of the personal data processed (e.g. pseudonymisation, use of work equipment, obligation to follow instructions) If a contractor carries out a survey, outbreak investigation or other epidemiological analysis (i.e. as data processors), the contractor are committed to the standard data protection obligations set out in the relevant procurement contracts (e.g. purpose limitation, obligation to follow instructions, processing mainly in EU/EEA) Risk level: limited As additional, medium-term mitigation measures, the controller is advised to: • conclude Terms of Reference with the organisations (public health authorities, clinics, academia) that provide case-based and contact-tracing data via REDCap and Go.Data. • consider adopting an instructional document governing outbreak investigations, preparedness evaluations and other epidemiological analysis. •
Purpose limitation	Terms of Service have been drafted to cover the use of the tools and related data protection aspects. Contractual provisions are in place to govern handling of data by external contractors. There is regular awareness raising and training on data protection principles and ICT security provided to ECDC staff. Access to REDCap

	and Go.Data is controlled and limited to nominated users. Risk level: negligible to limited

V. Conclusion

Based on the analysis above, it appears appropriate measures and safeguards have been put in place to protect the personal data. Whilst the processing involves sensitive health data, the risk posed to data subjects stemming from the processing of their personal data protection is limited. Indeed, identification of particular individuals is extremely unlikely based on the restrictions imposed on extent of data to be collected and shared, and other safeguards, including pseudonymisation and deletion after 1 year after the completion of the project, provided for. Both the terms of service and the procurement contracts provide for further protection. ECDC is transparent about this processing operation. It will publish the privacy statement and this DPIA, thereby making best efforts to inform all data subjects.

The purpose of the processing is legitimate and in accordance with ECDC's mandate.

Consequently, ECDC shall continue the processing operation. No prior consultation with the European Data Protection Supervisor is needed.