DPIA METHODOLOGY

GENERAL GUIDELINES : You will complete this DPIA in 4 steps.
- **1st step: Fill in Section A ("Knowledge Base") with information about your processing operation. Send this part to DPO for review, before completing the rest of the form.**
- **2nd step: Following approval from DPO, based on the information of the Knowledge Base, answer the questions in the so called "DPIA Template". In Section B ("Impact assessment") you will be asked to assess and rate various Data Protection risks.**
- **3rd step: Based on the answers you provided in Section B, you will describe in Section C ("Risk treatment") which measures you envisage to address the risks.**
- **4th step: Eventually, you will then give a general conclusion in Section D about the Data Protection Impact of your operation.**

Section A - KNOWLEDGE BASE

PART I - DESCRIPTION OF THE ENVISAGED PROCESSING OPERATION

This part is meant to provide a general overview of the envisaged processing operation.
The different steps you will identify within the processing operation will serve as a base to fill in the risk assessment and the necessity and proportionality assessment.

Flowchart

What do we collect - remember only to include details on sensitive personal data such as case-based health data	From where / whom	What we do with it	Where do we keep it	Who we give it to - include details both of ECDC staff who will have access and also any other recipients e.g. contractors, other agencies, WHO etc
pseudonymised personal data of study participants (incl. COVID-19 diagnosis, laboratory result, vaccination status, med. pre-condition, age, gender, socio-economic status, country of residence, occupation).	Data are collected from the study sites (e.g., hospitals, primary care settings, long-term care facilities, other health care providers). Sometimes, the information can be collected from the registry of health-related systems, or sometimes, they are first collected with paper based questionnaires. The study group are COVID-patients, patients with other infectious diseases and healthy individuals (e.g., health-care	Statistical analyses are performed in order to respond to the objectives of the study, namely to assess the vaccine effectiveness and the impact of the vaccination programmes.	Personal data are pooled and stored on the database of the contractor. The contractor will transfer the data to ECDC's epidemiological databases.	The data that are part of this study will be shared with selected staff of ECDC and Epiconcept on a need-to-know basis. Personal data transferred to ECDC's epidemiological databases will be shared with other authorised users on a need-to-know-bases. Access to the data stored in the epidemiological databases may be granted based on Regulation (EC) No. 1049/2001 on public access to documents.

Detailed description of the purpose(s) and supporting assets

Your process may include the following steps. Please only fill in the blanks for the steps that are included in your process.	Description of the process	Description of the purpose Please distinguish between purposes when necessary.	Supporting assets Please refer to the typology of supporting assets provided below and indicate for each step you identified which are the supporting assets (see section below for examples of supporting assets.)
Collecting of the data	web-based data collection methods or paper based methods can be used. Identifiers such as name, addresses and medical registration codes are deleted before the data transmission to the contractor. They are also not received by ECDC.	obtaining set of data for scientific evaluation of vaccine effectiveness and impact;	contractor's database and ECDC's surveillance databases
Merging datasets	collection of data form medical records or genetic databases	improving quality of data, e.g. by obtaining information about medical precondition and/or variants of the pathogen;	database of the study site and of other healthcare providers and public health authorities
Organising/structuring the data	Variables are recoded and new variables generated. Each record is given a country code, a hospital code and a unique number generated by the contractor	preparation of scientific analysis and optimisation of data collected;	contractor's database and ECDC's surveillance databases; statistical software;
Retrieving/consulting/using the data	Use of statistical software to perform analys	conducting scientific analysis of the data;	contractor's database and ECDC's surveillance databases; statistical software;
Editing/altering the data	Cleaned and edited databases are stored separately from the initial database	ensure update and accuracy of personal data;	contractor's database and ECDC's surveillance databases; statistical software;
Disclosing/transferring the data	Data is collected at country level and then transferred to contractors database via a secure data transfer system (two methods; a secure data transfer platform or data entry directly into a secure software); disclosure of pseudonymised case-based data to ECDC's stakeholders;	transferring data from (sub-)processors to ECDC for analysis; ensuring research analysis by ECDC's stakeholders;	secure data transfer system (two methods; a secure data transfer platform or data entry directly into a secure software);
Restricting the access to the data	n/a	n/a	n/a
Storing the data	Any subsequent change to the data is stored separately from the initial database.	ensuring availability of data for analysis;	ECDC's epidemiological database on premises;
Erasing/destroying the data	Personal data will be deleted or anonymised after retention period has lapsed.	ensuring storage limitation;	ECDC's epidemiological database on premises;
Other			

Interaction with other processes

Does this process rely on personal data being fed in from other systems? (Y/N)	Yes (partially)	Are data from this process re-used in other processes? (Y/N)	Yes (by transmission to ECDC's epidemiological databases)

KNOWLEDGE BASE FOR THE DESCRIPTION OF SUPPORTING ASSETS
Typology of supporting assets

Information systems	Hardware and electronic data media	Example: Computers, communication relays, USB drives, hard drives
	Software	Example: Operating systems, messaging, databases, business application
	Computer channels	Example: Computer channels: Cables, Wi-Fi, fiber optic
Organisations	People	Example: Users, IT administrators, policymakers
	Paper documents	Example: Print, photocopies, handwritten documents
	Paper transmission channels	Example: Mail, workflow

PART II - KNOWLEDGE BASE TO FILL THE TEMPLATE

Rating likelihood

1 : Negligible	2 : Limited	3 : Significant	4 : Maximum
It does not seem possible that the data protection principle (fairness, transparency, etc.) could be affected .	It seems difficult that the data protection principle (fairness, transparency, etc.) could be affected .	It seems possible for the data protection principle (fairness, transparency, etc.) to be affected .	It seems extremely likely that the data protection principle (fairness, transparency, etc.) would be affected.

Rating impact

1 : Negligible	2 : Limited	3 : Significant	4 : Maximum
Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome
Examples	**Examples**	**Examples**	**Examples**
Physical : classical negligible physical impacts include lack of adequate care for a dependent person (minor, person under guardianships), transient headaches...	**Physical** impacts : minor illness, lack of care leading to a Minor but real harm, Defamation resulting in physical or psychological retaliation	**Physical** impacts : Serious physical ailments causing long-term harm, Alteration of physical integrity (following an assault, an accident at home, work, etc.)	**Physical** impacts:Long-term or permanent physical ailments (e.g. due to disregard of contraindications), Death , Permanent impairment of physical integrity
Material impacts : - Loss of time in repeating formalities or waiting for them to be fulfilled - Receipt of unsolicited mail (e.g. spams) - Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing) - Targeted advertising for common consumer products	**Material** impacts : - Unanticipated payments (e.g. fines imposed erroneously), - Denial of access to services, blocked account - Lost opportunities of comfort (i.e. cancellation of leisure, termination of an online account) - Missed career promotion - Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects - Cost rise (e.g. increased insurance prices) - Non-updated data (e.g. position held previously) - Processing of incorrect data creating malfunctions - Targeted online advertising on a private aspect that the individual wanted to keep confidential - Inaccurate or inappropriate profiling	**Material** impacts: - Non-temporary financial difficulties (e.g. obligation to take a loan) - Targeted, unique and non-recurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban) - Prohibition on the holding of bank accounts - Damage to property - Loss of housing, Loss of employment - Separation or divorce - Financial loss as a result of a fraud (e.g. after an attempted phishing), Misappropriation of money not compensated - Blocked abroad	**Material** impacts: - Financial risk - Substantial debts - Inability to work - Inability to relocate - Loss of evidence in the context of litigation - Loss of access to vital infrastructure (water, electricity)
Moral impacts: - annoyance caused by information received/requested - Fear of losing control over one's data - Feeling of invasion of privacy without real or objective harm (e.g. commercial intrusion) - Lack of respect for the freedom of online movement due to the denial of access to a commercial site	**Moral** impacts : - Refusal to continue using information systems - Minor but objective psychological ailments (defamation, reputation) - Relationship problems with personal or professional acquaintances (e.g. image, tarnished reputation) - Feeling of invasion of privacy without irreversible damage - Intimidation on social networks	**Moral** impacts: - Serious psychological ailments (depression, phobia) - Feeling of invasion of privacy with irreversible damage - Feeling of vulnerability after a summons to court - Feeling of violation of fundamental rights - Victim of blackmailing - Cyberbullying	**Moral** impacts : - Long-term or permanent psychological ailments - Criminal penalty - Abduction - Loss of family ties - Inability to sue - Change of administrative status and/or loss of legal autonomy (guardianship)

DPIA Template

SECTION B - IMPACT ASSESSMENT

PART I. - Necessity and Proportionality Assessment

Necessity Need for the processing in order to achieve the aims assigned to the organisation		Proportionality Ensure that advantages resulting from processing are not outweighed by the disadvantages that processing causes			
How and why are the proposed processing operations an effective means for your organisation to fulfil the mandate assigned to it?	Have you considered alternatives for fulfilling this task? Why is the chosen approach the least intrusive one?	Benefits of the processing	Risks to the fundamental rights arising from the processing		
			Risk	Likelihood (rate from 1 to 4, see knowledge base)	Impact (rate from 1 to 4, see knowledge base)
ECDC has been commissioned by the European Commission to monitor the benefits and risks of vaccines and vaccinations, at EU level, including through post-marketing surveillance studies (Paragraph 10 and 11 Council's recommendation 2018/C	Personal data are needed in order to respond to the scientific questions related to vaccine effectiveness and impact of vaccination programmes. Data collected at EU level from a	scientific outputs on effectiveness of different vaccines	breach of confidentiality	2	3

(Paragraph 19 and 21 Council's recommendation 2018/C 466/01). The aims is to coordinate and to support national efforts via data and information sharing (Communication from the Commission to the European Parliament and the Council of 15 October 2020 on Preparedness for COVID-19 vaccination strategies and vaccine deployment, COM (2020)680 final). The scientific outcome of these studies will support vaccination policy related decisions.	programmes. Data collected at EU level from a number of Member States allow more accurate and representative results.	scientific output on impact of vaccination programmes	misuse of health data	2	2
		capacity building for Member States on response to public-health threats	breach of integrity and accuracy	2	1
		scientifically support to policy decision on vaccination			

Please rate the overall necessity of the process from 1 (redundant) to 4 (imperative)	Please rate the overall proportionality of the process from 1 (disproportional) to 4 (imperative)
4	3

PART II. - Risk Assessment: Assessing likelihood & impact

For each step of the processing operation (collection of data, merging data sets, etc.), answer *Yes/No* to the questions about the principles of data protection that they may affect.
Your processing operation may not involve all the steps that are linked to a question, or may include additional steps, which you can indicate in "other" : **please refer to the information you provided in Part I of the Knowledge Base to see which are the steps of your specific processing operation. To rate the possible impact of the process on each of the 7 data protection principles, please refer to Part II of the Knowledge base.**

I. Fairness

Questions	Step of the operation (Only answer (Yes/No) to the steps included in your processing operation)					
	Collection	Merging datasets	Retrieval/ consultation/use	Disclosure/ Transfer	Storage	Comments
1. Is the processing of this data something that people can expect, even without reading the information that you give them ?	Yes	Yes	Yes	No	Yes	Clinical studies are common, publicly known and socially accepted.
2. Consent (Remember that in the majority of cases ECDC relies upon doing a task in the public interest as the applicable legal basis, so consent may not be relevant here!) a. If you rely on consent, is it really freely given?	Yes	Yes	Yes	Yes	Yes	
b. If you rely on consent, can people revoke it?	Yes	Yes	Yes	Yes	Yes	
Please indicate how.	by contacting their local supervisory authority	by contacting their local supervisory authority	by contacting their local supervisory authority	by contacting their local supervisory authority	by contacting their local supervisory authority	The supervisory authority will contact the contractor and the latter ECDC.
c. If your processing operation relies on consent, please indicate how you document that people gave it. **If it relies on a legal obligation, internal rules or other,** please indicate which (for example, the Founding Regulation, Decision 1082, Financial Regulation etc - DPO can advise if unsure here)	Study sites provide participants with consent notes. Legal basis: Paragraphs 10 and 11 Council's recommendation 2018/C 466/01;	Study sites provide participants with consent notes. Legal basis: Paragraphs 10 and 11 Council's recommendation 2018/C 466/01;	Study sites provide participants with consent notes. Legal basis: Paragraphs 10 and 11 Council's recommendation 2018/C 466/01;01;	Study sites provide participants with consent notes. Legal basis: Paragraphs 10 and 11 Council's recommendation 2018/C 466/01;01;	Study sites provide participants with consent notes. Legal basis: Paragraphs 10 and 11 Council's recommendation 2018/C 466/01;01;	
3. Could this operation decrease the likelihood that people exercise their fundamental rights (e.g. freedom of expression, belief...) ? E. g. When investigating e-mails, if one checked the content instead of only checking the traffic data, this would decrease the likelihood that people exercise their freedom of expression.	No	No	No	No	No	It seems very unlikely that people will be dissuaded to seek medical treatment.
4. Could this processing operation lead to discrimination ?	No	No	No	No	No	
5. Is it easy for people to exercise their rights to access, rectification, erasure, etc. ?	Yes	Yes	Yes	Yes	Yes	Epiconcept and study sites have standard procedures for providing information in place.

Based on your answers, assess the **likelihood that a Data Subject would be affected by an unfair processing of his/her data** (rate from 1 to 4)	Based on your answers, **assess the impact if a Data Subject were affected** (rate from 1 to 4)
1	1

II. Transparency

Questions	Step of the operation (Only answer (Yes/No) to the steps included in your processing operation)						
	Collection	Merging datasets	Retrieval/ consultation/use	Editing/Alteration	Disclosure/ Transfer	Storage	Comments
1. Is the information you provide complete and easy to understand?	Yes	Yes	Yes	Yes	Yes	Yes	
2. Do you make sure the information you provide actually reaches the individuals concerned ? Answer Y/N and indicate how.	Yes	Yes	Yes	Yes	Yes	Yes	information notice provided to study participants by study site;
3. In case you defer informing people, please indicate how you justify this.	N/A	N/A	N/A	N/A	N/A	N/A	

Based on your answers, assess the **likelihood that a Data Subject would be affected by an untransparent processing of his/her data** (rate from 1 to 4)	Based on your answers, **assess the impact if a Data Subject were affected** (rate from 1 to 4)
1	1

III. Purpose limitation

Questions	Step of the operation (Only answer (Yes/No) to the steps included in your processing operation)								
	Collection	Merging datasets	Organisation/ structuring	Retrieval/ consultation/use	Disclosure/ Transfer	Restriction	Storage	Erasure/ Destruction	Comments
1. Have you identified all purposes of your process?	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	
2. Are all purposes compatible with the initial purpose?	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	The overall goal is to obtain new and accurate scientific insights.
3. Is there a risk that the data could be reused for other purposes ?	Yes	Yes	Yes	Yes	Yes	N/A	Yes	No	Contingent risk of re-use of personal data for commercial purposes.
Please indicate how you ensure that data are only used for their defined purposes e.g. via contractual provisions, terms of reference, clear instructions to staff, compliance with ECDC mandate etc.	strict policy on access to epidemiological databases; trainings for staff; contractual obligations;	individual authorisation of staff; strict policy on access to epidemiological databases; contractual obligations;	individual authorisation of staff; strict policy on access to epidemiological databases; contractual obligations;	individual authorisation of staff; strict policy on access to epidemiological databases; contractual obligations; ICT security policy (e.g., keeping logs); certification of processor;	contractual obligations; strict policy on access to epidemiological databases; procedure for 3rd party requests;	N/A	data stored in EU only; pseudonymise-tion; certification of processor; strict policy on access to epidemiological databases; contractual obligations;	pseudonymisation; retention period; ICT security policy;	
4. In case you want to re-use data for scientific research, statistical or historical purposes, do you apply appropriate safeguards ? (e.g. anonymisation or pseudonymisation)	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	

Please indicate which safeguards you apply.	All personal data are pseudonymised by default	All personal data are pseudonymised by default	All personal data are pseudonymised by default	All personal data are pseudonymised by default	All personal data are pseudonymised by default	N/A	All personal data are pseudonymised by default	All personal data are pseudonymised by default	

Based on your answers, assess the **likelihood that a Data Subject would be affected by a default of purpose limitation** (rate from 1 to 4)	Based on your answers, **assess the impact if a Data Subject were affected** (rate from 1 to 4)
2	2

IV. Data minimisation

Questions	Step of the operation (Only answer (Yes/No) to the steps included in your processing operation)						
	Collection	Merging datasets	Organisation/ structuring	Editing/Alteration	Disclosure/ Transfer	Restriction	Comments
1. Do you only collect data you need to achieve your goal ?	Yes	Yes	Yes	Yes	Yes	N/A	Based on the current knowledge, ECDC is collecting as much data as necessary. It is planned to reduce the set of necessary data.
2. Are there data items you could remove/mask without compromising the purpose of the process?	No	No	No	No	No	N/A	On a regular basis, ECDC shall re-evaluated which data do not provide essential information to respond to the question of vaccine effectiveness and impact of vaccination programme. These data will not be collected
3. When you collect data, for instance in forms, do you clearly distinguish between mandatory and optional information ?	Yes	Yes	Yes	Yes	Yes	N/A	
4. If you want to keep information for statistical purposes, do you appropriately manage the risk of re-identification? Answer Y/N and indicate how.	Yes, pseudonymisation by default; anonymisation of statistical reports	Yes, pseudonymisation by default; anonymisation of statistical reports	Yes, pseudonymisation by default; anonymisation of statistical reports	Yes, pseudonymisation by default; anonymisation of statistical reports	Yes, pseudonymisation by default; anonymisation of statistical reports	N/A	

Based on your answers, assess the **likelihood that a Data Subject would be affected by a default of data minimisation** (rate from 1 to 4)	Based on your answers, **assess the impact if a Data Subject were affected** (rate from 1 to 4)
1	3

V. Accuracy

Questions	Step of the operation (Only answer (Yes/No) to the steps included in your processing operation)							
	Collection	Merging datasets	Organisation/ structuring	Retrieval/ consultation/use	Editing/alteration	Disclosure/transfer	Restriction	Comments
1. Are the data of sufficient quality for the purpose?	Yes	Yes	Yes	Yes	Yes	Yes	N/A	established scientific standards apply.
2. Do your tools allow updating/correcting data where necessary?	Yes	Yes	Yes	Yes	Yes	Yes	N/A	
3. Do you take sufficient measures to ensure the accuracy of data you collect yourself? Answer Y/N and indicate how.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4. Do you take sufficient measures to ensure that the data that you obtain from third parties is accurate, and do you review it? Answer Y/N and indicate how.	Yes; checks are put in place.	Yes; checks are put in place.	Yes; checks are put in place.	Yes; checks are put in place.	Yes; checks are put in place.	Yes; checks are put in place.	N/A	Data is validated at different levels of data collection through different methods, with immediate checks and subsequently checked for consistency and validity.

Based on your answers, assess the **likelihood that a Data Subject would be affected by the processing of inaccurate data** (rate from 1 to 4)	Based on your answers, **assess the impact and the consequences if a Data Subject were affected** (rate from 1 to 4)
1	2

VI. Storage limitation (Retention period)

Questions	Step of the operation (Only answer (Yes/No) to the steps included in your processing operation)				
	Retrieval/ consultation/use	Restriction	Storage	Erasure/ destruction	Comments
1. Is the retention period defined by EU legislation ?	No	N/A	No	No	
2. Can you distinguish retention periods for different parts of the data ?	Yes	N/A	Yes	Yes	
Please indicate the retention period.	10 years for ECDC	N/A	10 years for ECDC	10 years for ECDC	The processor will be instructed to delete the personal data as soon as their task has been completed.
3. Is it really necessary to keep data for this period with regard to the purpose ? Please indicate the purpose for retaining the data for this period.	Yes	N/A	Yes	Yes	The ten years period is necessary to evaluate the vaccine effectiveness over time.
4. If you cannot delete the data immediately after the retention period, can you restrict or block access to it ?	Yes	N/A	Yes	Yes	Access to data is restricted on a need-to-know basis.
5. Will your tools allow automated erasure at the end of the storage period ?	No	N/A	No	No	

Based on your answers, assess the **likelihood that a Data Subject would be affected by a default of storage limitation** (rate from 1 to 4)	Based on your answers, **assess the impact if a Data Subject were affected** (rate from 1 to 4)
2	2

VII. Security - if using a contractor or other third party, you may need their input

Questions	Step of the operation (Only answer (Yes/No) to the steps included in your processing operation)								
	Collection	Merging datasets	Retrieval/ consultation/use	Editing/alteration	Disclosure/ Transfer	Restriction	Storage	Erasure/ Destruction	Comments
1. Do you have a procedure to perform an identification, analysis and evaluation of the information security risks that could affect personal data and the IT systems supporting their processing?	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	ECDC carried out a DPIA and an ICT security assessment on the epidemiological databases where the study data are to be stored (see 2021-DPO-020).
2. Is your data security procedure effective to safeguard the rights and freedoms of private individuals? Do you, apart from the risks to your organisation, also take into account the consequences for the rights of the persons whose data you process?	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	see DPIA 2021-DPO-020
3. Do you have resources and staff with assigned roles to perform the risk assessment?	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	see DPIA 2021-DPO-020
4. Do you systematically review and update the security measures in relation to the context of the processing and the risks?	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	see DPIA 2021-DPO-021

Based on your answers, assess the **likelihood that a Data Subject would be affected by a breach of security in the processing of his/her data** (rate from 1 to 4)	Based on your answers, **assess the impact if a Data Subject were affected** (rate from 1 to 4)
2	2

SECTION C - RISK TREATMENT
Measures envisaged to address the risks (likelihood and impact)

Generic controls - if using a contractor or other third party, you may need their input here in order to complete this part of the DPIA

Preventive: Do you prevent risks from materialising?	Y/N	Detective: Do you monitor your processing operations in order to ensure that you quickly notice breaches?	Y/N	Repressive: Do you ensure that you have means in place to quickly end detected breaches?	Y/N	Corrective: Do you ensure that you have the means to undo or limit damage after the fact?	Y/N
Do you sufficiently raise awareness among staff to prevent unauthorised data sharing ?	Yes	Do you use logging operations and self- monitoring to detect data breaches or illicit use ?	Yes	Do you have procedures to correct inaccurate data ?	Yes	Do you keep backups, so you can revert to the status quo ante after systems have been compromised ?	Yes
Do you keep conservation periods and the amount of data collected to the minimum ?	Yes						
Do you have a user management that allows you to quickly deactivate access rights of persons who no longer have a need to know (e.g. because they changed jobs) ?	Yes	Do you keep track of when and how you informed people about the processing ?	No	Do you certificate revocation mechanisms to stop the use of compromised credentials ?	No	Do you inform your recipients after an unauthorised transfer and instructing them to delete the data ?	Yes
Do you segregate personal data so that breaches of confidentiality in one repository do not affect others ?	Yes						
Do you encrypt storage devices ?	No						

Controls by Data Protection Principle														
	Fairness		Transparency		Purpose limitation		Data minimisation		Accuracy		Storage limitation (retention period)		Security	
Residual impact and likelihood rates after mitigating measures	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood
	1(4)	1(4)	1(4)	1(4)	2(4)	1(4)	3(4)	1(4)	2(4)	1(4)	2(4)	2(4)	2(4)	2(4)
Examples of generic controls to mitigate these weaknesses; Please cross out if not applicable!	check allowed/expected use when re-using data-sets		~~Automatically notifying data subjects~~		~~Limiting export functionalities;~~ Policy on data use; limited access on a need-to-know-basis (Permission rules); Terms of Service; pseudonymisation; Avoiding generic identifiers;		Collecting age ranges instead of birth dates; standard & mechanism on collection of data; constant review of collection of meta data;		Consistency checks; automated validation at ECDC and subsequent correction of personal data in ECDC's epidemiological databases; standard & mechanism on collection of Data quality reviews;		Distinguishing between conservation period for different parts of data; restricting access to relevant profile; retention period and automated anonymisation of patient data;		~~See EIB ISRM framework.~~ general ICT Security Policies; Certification of processor (ISO 27001:2013; Health Data Host); pseudonymisation; secured and restricts access (e.g. authentication, log keeping); secured network, systems and software; contractual obligations of processor, sub-processors and personnel; instruction and training for personnel; backup and disaster recovery plans in place;	
Other controls you propose to apply	Review of Data Protection Notification and DPIA regularly due to changing circumstances.		Publication of Data Protection Notification and DPIA on ECDC's webpage.				Continue reviewing the categories of the personal data processed with regard to the purpose.				request the processor to delete or anonymised personal data after the completion of the purpose.		Ensure that the legal basis applicable between controller, processor and sub-processors are compliant.	

SECTION D - CONCLUSION

Based on the knowledge base (Section A), on the results of the necessity and proportionality assessment (Section B, Part I .), on the impact and likelihood assessment (Section B, Part II) and on the risk treatment (Section C), please conclude about the overall impact of the process regarding personal data.

There is a necessity for scientific insights on the effectiveness and impact of vaccines in order to ensure that decisions on vaccination policies and strategies are based on evidence. These insights are also beneficial for citizens in order to take informed decisions on health care (e.g., on being vaccinated and the choice of the vaccine). The processing of personal data is thus necessary and proportionate.

Even though the processing operation involves health data, which is a sensitive category of personal data, the estimated risks to the rights and freedoms of the data subjects are overall low to limited. Data subjects are duly informed about the purpose and the means of data processing. Personal data are collected on the basis of strict scientific necessity. The processor is a certified Health Data Host experienced in that area. Personal data are exclusively processed in the EU. Contractual and organisational safeguards (e.g., policies and protocols) are in place. Access to personal data is granted on a need-to-know basis, secured and monitored. Systems, software and networks are protected by technical measures. The personal data stored at ECDC's epidemiological databases are pseudonymised.

As mitigating measures, the controller is advised to instruct the processor to delete or anonymise the personal data after the completion of the purpose and to publish the Privacy Statement and the DPIA on its webpage in order to further reduce the risks. In addition, the data collection policy shall be continuously reviewed and updated. Finally, it is recommended to ensure that the respective legal obligations between controller, processors and sub-processor are always clearly determined in appropriate legal instruments to be in place before processing operations are initiated.