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 caled "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 assesment 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
Identity contact data (e.g. name, user_ID, telephone numbers, password, etc.) and **content data** for OneDrive and backup.	From the **data subject** (i.e. the user).	Configuration of the **MS 365 core system setup** to enable other MS 365 Cloud services.	In segregated **Microsoft data centers in EU** (in Azure Activity Directories), in **ECDC's IT infrastructure** (In Active Directories, in OneDrive) and **Cloud Backup services**.	**ECDC staff and contractors** with administrator rights. **Contractors** with admin rights performing investigation under instructions from ECDC could also access data in special cases.

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	Identity contact data is collected from the users in form of onboarding process or changes during employment (via HR process). Content data is collected/managed by users themselves via uploading data to their OneDrive and via backup methods. Backup is furthermore done by IT operation as part of continuity routines.	Identity contact data is required to identify user rights and provide access control (authentication and authorisation). Content data is required to ensure availability of data for sharing and backup purposes.	MS OneDrive□ MS Intune MS Exchange Online MS SharePoint Online MS Project Online MS Dynamics 365 (SRM) MS Teams Cloud backup solution□
Merging datasets	eDiscovery and Search function in MS 365 cloud services.	Investigation of breaches.	n/a
Organising/structuring the data	Part of the Active Directories (AD) structure of data.	AD is the primary source of identity and access management in MS 365 cloud services.	Azure AD, Active Directory Federation Services (ADFS) and on-site AD
Retrieving/consulting/using the data	Built-in to MS 365 cloud services and eDiscovery and Search function.	Legal, IT operational, security and statistical reasons.	n/a
Editing/altering the data	Identity contact data could change if user change name, position or role (change general user information). Content data is managed by users themselves.	Request from user or HR to changes identity contact data or request from manager (of user) to change access rights for new role.	Azure AD, Active Directory Federation Services (ADFS) and on-site AD
Disclosing/transfering the data	Disclosure of data would only happen in case of investigation of breaches. Transfer of data should not taking place unless Microsoft (the processor) is transferring data un-announced.	In case of an investigation data may be disclosed to IT security Officer, Legal Services and/or the Director.	eDiscovery and Search function in MS 365 cloud services or via cloud backup service.
Restricting the access to the data	n/a	n/a	n/a
Storing the data	Identity contact data is stored in AD. Content data is stored in OneDrive and cloud backup service.	AD is the primary source of identity and access management in MS 365 cloud services. OneDrive and Cloud backup are primary storage for user documents.	Azure AD and on-site AD OneDrive (SharePoint) and Cloud backup service
Erasing/destroying the data	Built-in to MS 365 cloud services (retention functions).	Part of retention policies and based on Legal retention requirements.	MS 365 security center.
Other	n/a	n/a	n/a

Interaction with other processes

Does this process rely on personal data being fed in from other systems? (Y/N)	Yes - part of data entry by staff and IT administrators.	Are data from this process re-used in other processes? (Y/N)	No

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, WiFi, 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 outweighted 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	Likelyhood (rate from 1 to 4, see knowledge base)	Impact (rate from 1 to 4, see knowledge base)
Identity contact and content data is essential in order for ECDC to function in term of IT services. Using MS 365 cloud services encapsulate and process Identity contact and content data better/easier between the supporting assets. Cost efficient and added information security features are the primary reasons to invest in such services.	It is possible to use other cloud services (i.e. Google or Amazon) however (the data portection risks) processing of personal data would be the same for all type of cloud services. It is also possible to continue with an in-house solution; however it would probably be less cost-efficient and need large investment to have same type of security features.	Better collaboration	Misuse/abuse of personal data	2	3
		More security features	Data leak/breach or lack of control and audibility	2	2
		Better integration	Unauthorised access and processing (similar to misuse of data)	2	3
		Cost efficient	Vendor lock-in, lack of access and data	2	2

Who use the Cloud service	**Please rate the overall proportionality of the process** from 1 (disproportional) to 4 (imperative)
ECDC staff	3 (significant)

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 potection that they may affect.
Your processing operation may not involve all the steps that are linked to a question, or may include additionnal 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 whithout reading the information that you give them ?	No	N/A	Yes	Yes	Yes	The "Acceptable IT use" policy is always used.
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?**	N/A	N/A	N/A	N/A	N/A	
b. If you rely on consent, can people revoke it?	N/A	N/A	N/A	N/A	N/A	
Please indicate how.						
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)	N/A	N/A	N/A	N/A	N/A	
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	N/A	No	No	No	
4. Could this processing operation lead to discrimination ?	No	N/A	No	No	No	
5. Is it easy for people to exercise their rights to access, rectification, erasure, etc. ?	No	N/A	No	No	No	

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)
2 (limited)	2 (limited)

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?	No	N/A	No	No	No	No	How exact the MS 365 core functionality works is difficult to understand for standard users.
2. Do you make sure the information you provide actually reaches the individuals concerned ? Answer Y/N and indicate how.	Yes, (acceptable IT Use policy and HR processes)	N/A	Yes, (acceptable IT Use policy and HR processes)	Yes, (acceptable IT Use policy and HR processes)	Yes, (acceptable IT Use policy and HR processes)	Yes, (acceptable IT Use policy and HR processes)	
3. In case you defer informing people, please indicate how you justify this.	Pursuant to Art. 25 Reg. EU 2018/1725 deferrals due to investigation and inspection may apply.	N/A	Breaches according to the information security incident handling processes	Pursuant to Art. 25 Reg. EU 2018/1725 deferrals due to investigation and inspection may apply.	Pursuant to Art. 25 Reg. EU 2018/1725 deferrals due to investigation and inspection may apply.	Pursuant to Art. 25 Reg. EU 2018/1725 deferrals due to investigation and inspection may apply.	

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)
	2 (limited)

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	N/A	N/A	Yes	Yes	Yes	Yes	Yes	
2. Are all purposes compatible with the initial purpose?	Yes	N/A	N/A	Yes	Yes	Yes	Yes	Yes	
3. Is there a risk that the data could be reused for other purposes ?	No	N/A	N/A	No	No	No	No	No	
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.	Contractual framework (ILA and DP Addendum)	N/A	N/A	Contractual framework (ILA and DP Addendum)	Contractual framework (ILA and DP Addendum)	Contractual framework (ILA and DP Addendum)	Contractual framework (ILA and DP	Contractual framework (ILA and DP Addendum)	
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	N/A	N/A	Yes	Yes	Yes	Yes	Yes	
Please indicate which safeguards you apply.	Security controls according to policies	N/A	N/A	Security controls according to policies	Security controls according to policies	Security controls according to policies	Security controls according to policies	Security controls according to policies	

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 (limited)	3 (significant)

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	N/A	N/A	Yes	Yes	Yes	
2. Are there data items you could remove/mask without compromising the purpose of the process?	No	N/A	N/A	No	No	No	
3. When you collect data, for instance in forms, do you clearly distinguish between mandatory and optional information ?	No	N/A	N/A	No	No	No	All identity contact data is mandatory and content data is optional
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.	N/A	N/A	N/A	N/A	N/A	N/A	ECDC does not process personal data for statistical puroses.

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)
2 (limited);	2 (limited) for identity contact data; 3 (significant) for content data;

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	N/A	N/A	Yes	Yes	Yes	Yes	Content data is users responsibility .
2. Do your tools allow updating/correcting data where necessary?	Yes	N/A	N/A	Yes	Yes	Yes	Yes	
3. Do you take sufficient measures to ensure the accuracy of data you collect yourself? Answer Y/N and indicate how.	Yes	N/A	N/A	Yes	Yes	Yes	Yes	Need user training / awareness.
4. Do you take sufficient mesures to ensure that the data that you obtain from third parties is accurate, and do you review it? Answer Y/N and indicate how.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Do not obtain data from 3rd parties.

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)
2 (limited)	2 (limited)

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	No	No	No	Retention is an ECDC internal policy
2. Can you distinguish retention periods for different parts of the data ?	No	No	No	No	
Please indicate the retention period.	For as long as user is employed by ECDC	For as long as user is employed by ECDC	For as long as user is employed by ECDC	For as long as user is employed by ECDC	
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	Yes	Yes	Yes	
4. If you cannot delete the data immediately after the retention period, can you restrict or block access to it ?	Yes	Yes	Yes	Yes	Can disable user and hence block all data
5. Will your tools allow automated erasure at the end of the storage period ?	No	No	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 (limited)	2 (limited)

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

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	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Part of security risk management
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	N/A	Yes	Yes	Yes	Yes	Yes	Yes	
3. Do you have resources and staff with assigned roles to perform the risk assessment?	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	
4. Do you systematically review and update the security measures in relation to the context of the processing and the risks?	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	

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 (limited)	2 (limited)

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 ?	No	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 ?	Yes	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 ?	Yes						

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
	2/4	2/4	2/4	2/4	2/4	2/4	2/4	2/4	2/4	1/4	2/4	3/4	2/4	1/4
Exemples of generic controls to mitigate these weaknesses; Please cross out if not applicable!	Do not allowed re-using data- sets		Automatically notifying data subjects		Limiting export functionalities Avoiding generic identifiers		Limited data collection		Consistency checks		retention policy and automated anonymisation and erasure of personal data.		Audit event of MS 365 security configuration; Contractual provisions for EU location of Data Centres/Acquisition Process; Cryptographic Protection (keys managed by ECDC); Enforced access control for ECDC administrators; Identification and authentication procedures; Logging, alerting, and monitoring (both by IT security and CERT-EU staff); Security Awareness Training; Security Incident Handling procedures;	
Other controls you propose to apply	Data protection notification; Contractual provisions for EU location of Data Centres/Acquisition Process; Security Awareness Training		Data protection notification; Contractual provisions for EU location of Data Centres/Acquisition Process; Security Awareness Training		Contractual provisions for EU location of Data Centres/Acquisition Process; Role Based Security Training for IT staff		Security Awareness Training; Information Flow Enforcement of critical data (data loss prevention); Instructions for staff on use of OneDrive;		Security Awareness Training; Role Based Security Training for IT staff;		Implement retention policies in MS 365; Security Awareness Training;		Information Flow; Enforcement of critical data (data loss prevention); Information/knowledge Sharing between IT staff; Role Based Security Training for IT staff; System Security Plan (IT & Information security projects)	

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 likelyhood assessment (Section B, Part II) and on the risk treatement (Section C), please conclude about the overall impact of the process regarding personnal data.

MS 365 core is a fundamental part to pursuit a cloud strategy using Microsoft cloud services. The privacy and security risks for the data subjects are - generally speaking - limited. Many security safeguards are already in place to mitigate risks e.g. data encryption, audit events, access control, logging/monitoring and security incident handling. The contract with Microsoft is currently being re-negotiated by the European Commission and the outcome looks like an approval of the data protection requirements will happen.

Human errors are a risk with a significant impact. The impact of the risk can be significantly reduced by using classification of sensitive/private data, data loss presentation and security awareness/training campaigns. The current IT security policy already contains rules and instructions for staff regarding the acceptable use of IT equipment.

The usefulness of the MS 365 core outweighs the risks involved, given the current and proposed safeguards.