DTM Data Protection Checklists[1]

The below checklists are intended to be practical tools to assist DTM coordinators to ensure compliance with IOM's Data Protection Principles. They include key factors to be taken into account at the different stages of the DTM project. Please note that the checklists are not exhaustive and you should always consult the IOM Data Protection Manual for further guidance.

The checklists should be used **prior** to commencing a DTM project.[2]

RISK-BENEFIT ASSESSMENT[3]	YES	NO
Is it clear which of the data you will be collecting under this DTM project are personal data and which are non-personal data?		
Have you made a list of all the personal data you will be collecting from the data subjects[4] under this DTM project?		
Is it clear which is the specified and legitimate objective for the collection of those personal data?		
Have you considered whether all the personal data you are planning to collect are needed in order to fulfill the purpose of the specific project? (you need to ensure that you collect the minimum personal data possible to achieve the specific purpose)		
Have you clearly identified the following roles: data controller (staff who has the overall responsibility of the personal data and who provides instructions to the data processors on how to e.g. collect, use, store, share and destroy them) and data processor (staff who process the personal data according to the instructions of the data controller)?		
Have you conducted a risk-benefit assessment prior to the collection of the personal data?[5] (At a minimum, have you listed all the risks and benefits that arise from collecting the specific type of personal data from data subjects to achieve the specific purpose?)		
Do the benefits of collecting the specific types of personal data for the specific purpose outweigh the risks?		
Have you planned to review the risks on periodic basis to identify new potential risks?		
Have you planned to check on regular basis if the benefits still outweigh risks?		
SENSITIVITY-ASSESSMENT	YES	NO
Are all types personal data that will be collected properly classified according to the level of sensitivity applied to it? (i.e. low sensitivity, medium sensitivity, high sensitivity)		
Was the highly sensitive data identified? If yes, have you ensured that adequate safeguards are in place to protect such data?		

[1] These checklists are developed on the basis of the checklists included in MA/88 "IOM Data Protection Manual" and they are in line with the IN/138 "IOM Data Protection Principles". They are meant to be living documents and they may be amended from time to time. For any comments to the checklists please email sdaviot@iom.int

[2] If you have already commenced a DTM project, you can still go through the checklists to check if your project is compliant with IOM's Data Protection Principles and make changes as deemed appropriate.

[3] This checklist does not constitute the "Risk-Benefit Assessment" itself, which should be done separately. DOE and LEG are currently in the process of developing a template for conducting a risk benefit assessment. For any questions on how to conduct it for the time being please contact leg@iom.int

[4] The term « data subject » means an IOM beneficiary who can be identified directly or indirectly by reference to specific factor or factors. Such factors may include a name, an identification number, material circumstances and physical, mental, cultural, economic or social characteristics.

[5] See footnote 2.

Have you planned to properly mark the personal data as being of “low sensitivity”, “medium sensitivity” or “high sensitivity” after the data will be collected?		
Have you planned to review the sensitivity of data on regular basis?		
CONSENT		
Are you able to record the consent of each data subject in writing prior to collecting their personal data?		
If written consent is not possible to obtain prior to the collection of the personal data have you evaluated the moment when such consent can be sought?		
If written consent is not possible, are you able to record the consent in another way (e.g. audio recording)?		
If recording the consent is not possible, have you contacted LEG to ensure another basis of collecting the personal data?		
Is your environment safe to seek consent of each individual IOM beneficiary?		
Is personal data collected in non-intimidating manner, with due respect of dignity of the data subject?		
Do your data subject know what the specified purpose, related purposes and additional purposes of data collection are at the time of data collection?		
Have you been providing the data subjects with an accurate and fair description of the risks and benefits at the time of data collection?		
Have you considered the data subjects’ physical and mental capacity to consent (e.g. from vulnerable data subjects)?		
Have you explained to the data subject that IOM may disclose their personal data to third parties (including donors and project partners) and have you mentioned to them for which specific reason the personal data will be shared?		
Have you explained to the data subject that he/she has the right to contact IOM to access their personal data, request to modify and/or delete them?		
Have you ensured that the data subject has all necessary IOM contact information?		
CONFIDENTIALITY		
Is your staff briefed about the confidentiality of personal data prior to the collection, use and disclosure of such data?		
Do DTM staff know that in accordance with their contracts and the IOM Staff Regulations and Rules they are obliged to respect confidentiality?		
Do DTM staff know that the obligation of confidentiality continues even after the end of their employment with IOM?		
Are you applying strict access controls to the lists containing personal data of IOM beneficiaries and maintaining an access record of personal data disclosed?		
Are you ensuring that all transmission of personal data within IOM are secure, correspondence is highlighted as “secret” and the recipients of e-mails are carefully selected?		
Are you monitoring the disposal of printed copies and other paper trails containing personal data, including the shredding of printed material containing personal data?		
DATA SECURITY		
Have you analyzed the level of security at workstations according to sensitivity levels, confidentiality, integrity, transmission and access to data?		
Have you evaluated the storage location and safety measures needed to protect paper records?		

Have you evaluated the electronic storage areas and safety measures needed to protect electronic records, including backups?		
Have you ensured the proper management of electronic and paper records to prevent unauthorized retrieval?		
Have you enquired with ICT about the latest updates in information technology , including the availability of encryption software to be used when storing personal data?		
Have you ensured a limited access to personal data of IOM beneficiaries for certain categories of IOM staff, consultants and individuals?		
Have you ensured strict access control and maintenance of personal data disclosed?		
DATA QUALITY		
Have the data subjects validated the personal data they provided to IOM?		
Have you taken reasonable steps to verify the accuracy and truthfulness of personal data at the time of data collection?		
Are the DTM staff trained on data protection?		
Are the DTM staff trained on collecting personal data?		
Has the need for truthful personal data been emphasized and have the consequences of relying on inaccurate personal data been highlighted?		
Are electronic records containing personal data stored in safe media that are protected from security risks and unauthorized access and have regular backup procedures occurred?		
Are paper records containing personal data stored in safe locations to prevent wear and tear and unauthorized access?		
Has the quality of personal data been affected by any inaccuracies?		
Have updates to the personal data been accurately recorded in the electronic and/or paper records?		
Have you encouraged the practice of cross-checking prior to collecting personal data and prior-checking before use and disclosure of personal data?		
SHARING PERSONAL DATA WITH THIRD PARTIES		
Does the donor agreement for this DTM project include a provision stating that IOM will comply with its Data Protection Principles when processing personal data?		
Have you offered/counteroffered to share aggregate non-personal data?		
Have you ensured the consent of the data subjects to share their personal data with a third entity? This is mandatory.		
Is the specified purpose for which personal data will be shared clear?		
Have you contacted LEG for advice prior to transfer of personal data? It is mandatory to sign a written agreement when sharing personal data, so you have to contact LEG.		
Have you evaluated the existence of data protection legislation, compliance with data protection laws and regulations in the country of the third party?		
Have you limited the amount of the personal data to that which is necessary to achieve the specified purpose of transfer?		
Have ensured (in coordination with the ICT Officer) that the method of transfer is safe and secure?		