PHILIPLEE

DATA PROTECTION & HEALTH RESEARCH GUIDE TO DATA TRANSFERS

Anne Bateman, CIPP/E

14 July 2022

DATA SHARING AND DATA TRANSFERS
WHAT TO CONSIDER

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

Data Sharing and Data Transfers #1

- "Processing" of personal data/personal information by data controllers and data processers is what is regulated under the GDPR
- Remember the definition of "processing" is very wide – anything that can be done with personal information
- Includes sharing personal data and transferring personal data
- Remember difference between data controllers and data processors
- Recall the data protection rules from Part 1, including:-
  - Having a legal basis for the sharing and/or transfer (external/third parties)
  - Data minimisation (internal and external), e.g. pseudonymisation
  - Data security

Data Sharing and Data Transfers #2

- Data sharing usually refers to any sharing of personal data by a data controller or disclosure of personal data to third parties, usually with/to other data controllers
- Distinguish from data processing arrangements, which are separately governed by A.28 GDPR *(see more detail later)*
- For purposes of this seminar, data transfers refer to transfers of personal data to "third countries", i.e. countries outside the EEA (EU + Norway, Iceland and Liechtenstein)
- Note UK is outside EEA
- USA is also a "third country"

DATA SHARING – DATA PROCESSING AGREEMENTS

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

GDPR: data processing contracts #1

- Article 28 GDPR
- Article 28.1: Obligation on controller to vet processor's technical and organisational security measures + Article 30.2: processor must maintain certain records of its processing activities
- Article 28.3 GDPR: processing shall be governed by a contract or other legal act that is binding on the processor with regard to the controller
- Data processing contract must set out
  - Subject-matter and duration of the processing
  - Nature & purpose of the processing
  - Type of personal data concerned
  - Categories of data subject concerned
  - Obligations & rights of the controller

GDPR: data processing contracts #2

- Article 28.3 GDPR – goes on to set out very prescriptive requirements for the content of the controller-processor contract
- Supplemented by ***EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR*** (updated in July 2021), see: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf
- **NB:** New EDPB Guidelines (above) recommend more prescriptive and detailed contractual obligations than simple mirroring of obligations set out in A.28.3 GDPR
- Note: HSE has standard data processing and confidentiality agreement

GDPR: data processing contracts #3

- A.28.3 GDPR requirements to be imposed on processors:-
  - Process personal data only on documented instructions from the controller including regarding cross-border data transfers, subject to certain limited exceptions
  - Impose confidentiality obligations on all personnel authorised to process the personal data
  - Ensure the security of the personal data that it processes
  - Abide by the rules regarding appointment of sub-processors
  - Implement measures to assist the data controller in complying with data subjects' rights

GDPR: data processing contracts #4

- Assist the controller with the controller's compliance obligations under Article 32 (security arrangements for processing), Article 33 (data breach notifications), Article 34 (communicating data breaches to individuals), Article 35 (conducting data protection impact assessments) and Article 36 (consultations with data protection regulatory authorities prior to engaging in risky processing activities)
- At the controller's election, either return or destroy the personal data at the end of the relationship, unless EU or member state law requires a longer retention period.
- Provide the controller with all information necessary for the data controller to demonstrate compliance with the GDPR's obligations relating to engaging data processors. The data processor must notify the data controller immediately if it believes that any instructions from the data controller to provide information violate the GDPR or any other EU or local law.
- Allow for and contribute to audits, including inspections, by the controller

GDPR: data processing contracts #5

- Sub-processing contracts must reflect the Article 28.3 requirements:-
  - Impose same requirements on sub-processor as are on the main processor
  - Ensure sub-processor does not process personal data except on instructions from data controller
- Specific requirements for engaging sub-processors:-
  - Main processor must be pre-authorised, in writing, to engage sub-processors, either generally or specifically (i.e. reference to specific sub-processors)
  - If the written pre-authorisation is general, main processor must advise controller of any changes to its sub-processors and give the controller the right to object to the changes
- Main processor remains liable for sub-processors (A.28.4 GDPR)

DATA SHARING – CONTROLLER TO CONTROLLER AGREEMENTS & JOINT CONTROLLER AGREEMENTS

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

Controller/Joint Controller Agreements

- No specific contractual obligations in GDPR
- Wise to document terms for data sharing in formal agreement or MOU
- Sometimes the DP-related legal obligations can be as little as *"each controller will comply with their own obligations under data protection law"*
- For joint controllership, GDPR obligations are more specific
- A26 GDPR requires joint controllers to determine and document their respective obligations, e.g. ref individuals' rights, and make this available to individuals

DATA TRANSFERS OUT OF THE EEA

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

Data Transfers ex-EEA #1

- Transferring data out of the EEA is prohibited under current data protection rules and under the GDPR, unless specific conditions apply
- Permissible conditions for transfer are set out in the GDPR
- Note that transfers can include not just transferring out data physically or electronically to a country outside the EEA, but also permitting a person located outside the EEA to access data that are located within the EEA
- A.44 GDPR = key provision: in relation to any personal data that is proposed to be transferred, the level of protection of individuals guaranteed under the GDPR is not undermined
- Means – protection in recipient country must be essentially equivalent

Data Transfers ex-EEA #2

- **Option 1 – A.45 GDPR**
- Recipient country offers an adequate level of protection for personal data (as determined by EU Commission in a formal adequacy decision)
- Standard = essential equivalence of protection
- If adequacy decision in place, EU controller/processor can transfer without further condition (but must continue to comply with other GDPR obligations, e.g. data minimisation, data security)
- Adequacy decisions: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (includes UK, but does not include USA)

Data Transfers ex-EEA #3

- **Option 2 – A.46 GDPR**
- Appropriate safeguard mechanisms, subject to assessment of appropriate levels of protection by transferring EU controller/processor
- Mechanisms (mainly contractually-based):-
  - Standard Contractual Clauses (SCCs, most common in Ireland)
  - Binding Corporate Rules (BCRs) (inter-group transfers in private sector)
  - Codes of Conduct (none in Ireland yet)
  - Certification Mechanisms (none in Ireland yet)
  - Ad Hoc Contractual Clauses

Data Transfers ex-EEA #4

- **Standard Contractual Clauses** (or **EU Model Clauses**)
- GDPR versions adopted by EU Commission in June 2021, available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en
- 4 options ("modules"):-
  - Transfer controller to controller
  - Transfer controller to processor
  - Transfer processor to processor
  - Transfer processor to controller

Data Transfers ex-EEA #5

- Model clauses are very detailed: can be used stand-alone or as part of a wider agreement (e.g. as a separately signed schedule)
- No material amendment, else will require regulatory approval
- Old SCCs (approved under DPD 1995) concluded prior to 27 Sept 2021 can be used up to 27 Dec 2022

Data Transfers ex-EEA #6

- **BUT!** Not as simple as signing SCCs or using other transfer mechanisms
- CJEU reviewed validity of SCCs in **Schrems II** case (decision in July 2020)
- Case originally concerned with examining validity of the EU-US Privacy Shield (an additional mechanism under A.46 GDPR) - invalidated as violating EU DP law, because of insufficient guarantees of data protection for data in USA (US surveillance laws) – level of protection not essentially equivalent
- The predecessor to Privacy Shield (Safe Harbour Agreement) was struck down by the CJEU in October 2016, on similar basis (**Schrems I case**)

Data Transfers ex-EEA #7

- **Schrems II** decision means that EU data exporters using SCCs must:-
- **1.** Verify, on case-by-case basis, whether law in intended recipient country ensures essentially equivalent level of protection for the personal data
- Particularly insofar as powers of public authorities to access and surveil the personal data
- **2.** If necessary, provide for supplementary measures (to those contained in SCCs) to guarantee essentially equivalent protection for the personal data
- **3.** Otherwise, do not proceed with or (as applicable) suspend the data transfers

Data Transfers ex-EEA #8

- European Data Protection Board (EDPB) Recommendations: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (Version 2.0, June 2021)
  - **Step 1**: Know your transfers – what transfers are proposed/taking place? what personal data? for what purpose(s)? Consider data minimisation, security and other obligations (encryption, pseudonymisation) (**DPIA**)
  - **Step 2**: What transfer tools are being relied upon? EU Commission Adequacy Decision? A.46 GDPR mechanism, e.g. SCCs?
  - **Step 3**: Is the transfer tool (e.g. SCCs) adequate in all the circumstances? Examine EDPB European Essential Guarantees (EEG) ref risks (https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en)

Data Transfers ex-EEA #9

- **Step 4**: Adopt supplementary measures (if transfer tool is not effective) (Contractual, technical, organisational – examples set out in Annex 2 of EDPB Recommendations, but also describes issues that would disqualify those examples)
- Ref. contractual – knit into contract obligations on data recipient (supplementary to SCCs)
- **Step 5**: If can identify effectively/suitable supplementary measures to implement, need to take further procedural steps (e.g. notification / approval from data protection supervisory authority)?
- **Step 6**: Re-evaluate at appropriate intervals – developments in recipient country that could cause reassessment of risk to personal data and/or assessment of essential equivalence; have mechanism for promptly suspending transfers if necessary

Data Transfers ex-EEA #10

- **Option 3 – A.49 GDPR**
- Specific derogations, e.g. individuals have explicitly consented to the transfer; transfer is necessary for performance of a contract; transfer necessary for establishment, exercise or defence of legal claims
- Derogations are for exceptional use (interpreted restrictively), and in some cases are restricted to occasional, non-repetitive transfers
- EDPB Guidance on A.49 GDPR derogations: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

Practicalities in Health Research Context

- Remember under DPHRR, either need an "***assessment of data protection implications of the health research***" or (if high risks to individuals) a **DPIA**
- DP Assessment / DPIA will reveal details of data processing, data sharing and data transfers involved in research project
- Specific compliance measures (apart from data minimisation, etc.):-
  - Data Processing: Security Audits/Assessments + Data Processing Agreements (processors and sub-processors)
  - Data Sharing (Controllers / Joint Controllers): Data Sharing Agreement (or data sharing Ts+Cs incorporated into wider agreement)
  - Data Transfers: GDPR-compliant transfer mechanism (e.g. SCCs)

SECONDARY USE OF HEALTH DATA
REVIEW OF CURRENT RULES

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

Primary –v- Secondary Use of Health Data

- **Primary use** of health data generally refers to collection and use for **medical treatment** and part of patient's health record
- Health data can also be directly collected from patients expressly for health research purposes – GDPR rules apply directly, e.g. legal basis, transparency, etc.
- **Secondary use** of health data generally refers to use of **existing stored health data for other purposes**, including **later health/medical research**
  - E.g. Existing patient records in hospital or GP surgery
  - E.g. Existing/historic health screening or vaccination records
- Normal GDPR rules and how impacted by Data Protection (Health Research) Regulations 2018 (amended in 2019 and 2021) (**DPHRR**)

Reminder: “health research” under DPHRR #1

- “Health research” as defined by DPHRR, neutral on purpose, covers secondary use

(i) research with the goal of understanding normal and abnormal functioning, at molecular, cellular, organ system and whole body levels
(ii) research that is specifically concerned with innovative strategies, devices, products or services for the diagnosis, treatment or prevention of human disease or injury
(iii) research with the goal of improving the diagnosis and treatment (including the rehabilitation and palliation) of human disease and injury and of improving the health and quality of life of individuals
(iv) research with the goal of improving the efficiency and effectiveness of health professionals and the health care system
(v) research with the goal of improving the health of the population as a whole or any part of the population through a better understanding of the ways in which social, cultural, environmental, occupational and economic factors determine health status

Reminder: “health research” under DPHRR #2

- “Health research” includes action taken by data controller to establish whether an individual may be suitable or eligible for inclusion in the research, but this activity may not require “explicit consent” if conditions contained in the DPHRR 2021 Amendment Regulations apply
- Also, requirement for explicit consent in DPHRR not apply to retrospective chart reviews approved by research ethics committee where the committee certifies that the data protection implications of the processing indicates a low risk to the rights and freedoms of individuals
- Other conditions of DPHRR (suitable and specific measures) will apply to retrospective chart reviews
- Clinical reviews may not be subject to DPHRR depending on purpose
- Health research –v- statistical compilation (latter subject to separate conditions in GDPR)

Current DP rules for secondary use

- Otherwise, A.5(1)(b) GDPR (rule on purpose limitation): further processing of personal data for scientific research (e.g. health research) purposes will not be considered incompatible with the initial purpose for which the personal data were collected (e.g. primary use of health data), as long as A.89(1) GDPR is complied with
- A.89(1) GDPR requires safeguards for health research: TOMs, data minimisation
- BUT for "health research" as defined by the DPHRR, the default legal basis for any research (including secondary use) is explicit consent
- Operates as effective derogation to other available legal bases and conditions set out in Articles 6 and 9 GDPR for health research (even noting guidance on other more suitable legal bases set out by EU Commission and EDPB); derogation permitted under A.9(4) GDPR

Q&A / Thank you

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

PHILIPLEE

philiplee.ie
info@philiplee.ie

DUBLIN
7/8 Wilton Terrace
Dublin 2
Ireland
T: +353 (0)1 237 3700
F: +353 (0)1 678 7794

LONDON
2 Eastbourne Terrace
London, W2 6LG
United Kingdom
T: +44 (0)20 3934 7010
F: +353 (0)1 678 7794

BRUSSELS
39 Rue des Deux Eglises
1000 Brussels,
Belgium
T: +353 (0)1 237 3700
F: +353 (0)1 678 7794

SAN FRANCISCO
201 Spear Street, Suite
1100 CA 94105,
United States
T: +353 (0)1 237 3700
F: +353 (0)1 678 7794