Intro to the UK GDPR – including international data transfers

Guido Noto La Diega

University of Trento, October 2021

Overview

- Introduction to the UK legal system(s) – sources, human rights, interpretation, precedent
- Introduction to data protection – law and instutional framework
- International transfers – from the EEA and from the UK

Statutes and bills

- Legislation is a broad term which covers not only statutes (i.e. Acts of parliament) but other types of legislation such as delegated legislation (sometimes called subordinate legislation) and, until 1 January 2021, European legislation
- Parliament passes legislation in the form of statutes, or Acts of parliament. Such Acts will often begin as a Bill
- Government proposals on topics of current concern are set out in White Papers. These signify the government's intention to enact new legislation, and may involve setting up a consultation process to consider the finer details

Delegated legislation

- Parliament has delegated the power to legislate to various persons and bodies (ministers, local authorities, etc.)
- Delegated legislation is law made by such persons or bodies with the authority of Parliament.
  - This authority is granted by an enabling Act (a parent Act)
- Most notably, the statutory instruments: **regulations**, rules and orders adopted by the Ministers of the Crown
- Unlike Acts of parliament, delegated legislation may be challenged in the courts via the doctrine of ultra vires e.g. cfor incompatibility with the ECHR

Impact of the Human Rights Act 1998

Section 19 of the **Human rights Act** 1998 ('HRA 1998') provides that the Minister in charge of each new Bill in either House of parliament must, before the second reading of the Bill, either:

- make a **statement of compatibility** – that is, state that the provisions of the Bill are compatible with the European Convention on Human rights ('ECHR'); or
- make a statement acknowledging that it is not possible to make a statement of compatibility, but, despite this, **the government still wishes the House to proceed** with the Bill. This is typically done on the first reading.

Moreover, the **courts have no power to set aside any Act of parliament** that is incompatible with convention rights; this is the prerogative of parliament (the doctrine of **parliamentary sovereignty** means that the validity of any statute passed by parliament cannot be challenged)

Precedent and the HRA 19985

- Section 2 of the HRA1998 requires future courts to take into account any previous decision of the ECtHR
- Although these decisions are not formally binding, they are highly persuasive, which has major implications for the operation of the doctrine of precedent.
- The provision effectively allows the overruling of any previous case authority that was in conflict with a previous decision of the ECtHR (*R (on the application of H) v. Mental Health Review Tribunal for North and East London* [2002] QB 1, CA)

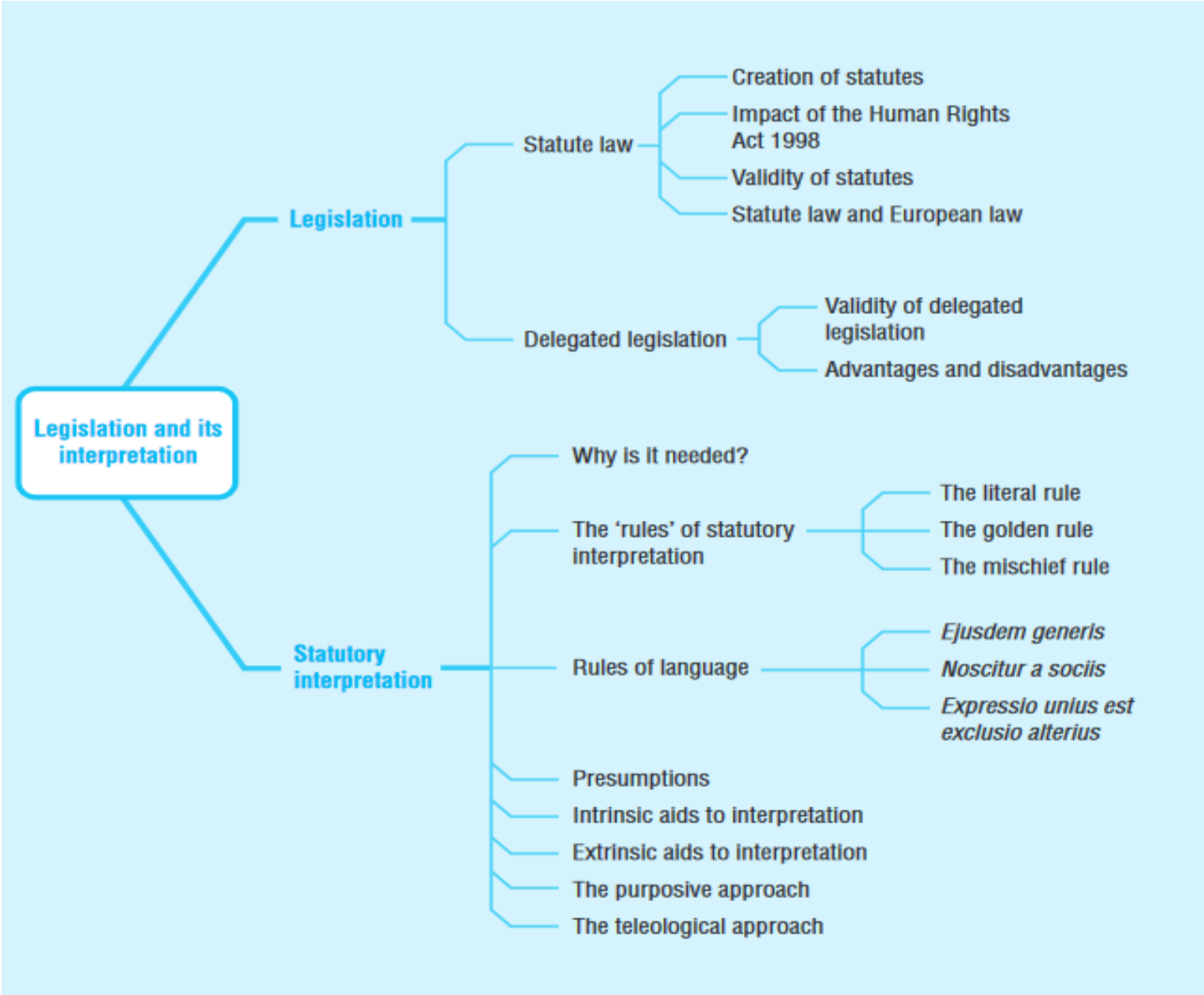
Impact on private relations – Convention compatible construction

- Whilst the HRA only applies directly against public authorities (pursuant to s 6), the impact of the HRA on private relations must not be ignored.
- By way of a process of indirect horizontal effect via s 6(3) HRA and a broadened out interpretation obligation under s 3, ECHR rights now have considerable applicability even in relation to both public and private relations
- S 3 sets forth a mandatory requirement that the Courts interpret primary and secondary legislation in a manner compatible with Convention rights "so far as it is possible to do so"

Statutory interpretation

- The words of an Act of parliament are authoritative. the constitutional role of the judiciary is the application of legislation. if the wording of the legislation is ambiguous or unclear, then its meaning will need to be interpreted
- The rules of construction:
  - Literal rule - words must be given their plain, ordinary and literal meaning (even if the outcome is harsh or undesirable, *Sussex Peerage Case* (1844) 1 Cl & Fin 85)
  - Golden rule - words must be given their plain, ordinary and literal meaning to the extent that they do not produce absurdity or an affront to public policy (*Grey v Pearson* (1857) 6 HL Cas 61, HL)
  - Mischief rule - an examination of the former law in an attempt to deduce Parliament's intention (*Heydon's Case* (1584) 3 Co Rep 7a)
  - Purposive approach - beyond the words used in the provision to find an interpretation which furthers its general purpose (predominant, *R (on the application of Quintavalle) v Secretary of State for Health* [2003] 2 Ac 687, HL)

Legislation and its interpretation



Case law is a source of law

- Common law is the body of customary law, based upon judicial decisions and embodied in reports of decided cases
- Another, narrower, sense, common law is contrasted to the rules applied in English and American courts of equity and also to statute law
- Doctrine of precedent: *stare decisis* means ‘let the decision stand’ which means that once a decision has been reached in a particular case, it stands as good law and should be relied upon in other cases as an accurate statement of law
- The doctrine of precedent is based on the principle that like cases should be treated alike. This preserves certainty and consistency in the application of the law.
- Adherence to the doctrine of precedent also ensures that the law is sufficiently flexible to deal with novel situations and to ensure justice in each particular case

Doctrine of precedent

The doctrine of precedent is based upon these presumptions:

- Cases with the same or **similar material facts** (facts which are legally relevant) should be decided in the same way
- Decisions made in the **higher level courts** carry greater weight than those lower in the hierarchy. A court is normally bound by courts which are higher or equal to them
- The legal reasons for the decision in the previous case (the ***ratio decidendi***) must be identified and followed. These are distinct from any comments made in passing which are peripheral to the outcome of the case (*obiter dicta*)

A **binding precedent** is one that (generally) must be applied in a later case because the facts of a case are analogous with those of an earlier decision in a higher or equivalent court in which the applicable statement of law was part of the ratio of the earlier decision. Otherwise it's *persuasive*

Data Governance in the UK

- **Data protection** – Data Protection Act 2018 (DPA 2018) incl. UK GDPR
- **Privacy and Electronic Communications** Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications. Specific rules for:
  - marketing calls, emails, texts and faxes;
  - cookies (and similar technologies);
  - keeping communications services secure; and
  - customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.
- **FOI** - Freedom of Information Act 2000 provides public access to information held by public authorities
  - Plus sector-specif data i.e. Environmental Information Regulations 2004 and INSPIRE Regulations 2009 on spatial data
- **Other**: eIDAS Regulations (legal framework for the use of electronic trust services e.g. e-signature); NIS Regulations 2018 (security for network and information systems of essential services and digital services providers e.g. online marketplaces, online search engines and cloud services); Re-use of Public Sector Information Regulations 2015 (permits use of public sector information for a purpose other than the initial public task it was produced for)
- **Common law**: breach of confidence and misuse of private information

Legislative references and data protection authority

- The UK data protection regime is set out in the Data Protection Act 2018 ('DPA 2018'), along with the UK General Data Protection Regulation ('UK GDPR')
- The Information Commissioner's Office ('ICO') is the equivalent of the Italian *Garante per la Protezione dei Dati Personali* ('Garante')
- The ICO regulates data protection in the UK, offers advice and guidance, promotes good practice, carries out audits, considers complaints, monitors compliance and takes enforcement action where appropriate
  - Also cooperates with data protection authorities in other countries, including the European Data Protection Board ('EDPB')
  - The current proposals for the Secretary of State to approve ICO guidance and to appoint the CEO do not sufficiently safeguard its independence

DPA 2018

The DPA 2018 sets out the data protection framework in the UK, alongside the UK GDPR. Replaces the DPA1998, came into effect on 25 May 2018, and was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018

It contains three separate data protection regimes:

- Part 2: sets out a **general processing regime** (the UK GDPR);
- Part 3: sets out a separate regime for **law enforcement** authorities ('LEAs'); and
- Part 4: sets out a separate regime for the three **intelligence services -** MI5, SIS (aka MI6), and GCHQ

Differences DPA/GDPR

- DPA sits alongside and supplements the UK GDPR - for example by providing exemptions (‘restrictions’)
  - *R (on the Application of The Open Rights Group & Anor) v The Secretary of State for the Home Department & Anor* [2021] EWCA Civ 800: The ‘immigration exemption’ contained in the DPA (sch 2, pt 1 [4]), which disapplied certain data protection rights for the purpose of maintaining effective immigration control, was incompatible with art 23 GDPR
    - Article 23(2) sets out a list of "*specific provisions*" that any legislative measure creating a restriction to data subjects' rights must contain e.g. purpose of the processing and safeguards to prevent abuse
  - March 2021, ICO guidance on the national security exemption in Part 2 of the DPA18
- Sets out separate data protection rules for LEAs
- Extends data protection to some other areas e.g. national security and defence
- Sets out the ICO’s functions and powers

The UK GDPR

- The UK GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 1 January 2021
- It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies
- It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context
  - Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ('EU Exit Regulations') applied a number of necessary changes to the GDPR to make it relevant to the UK following departure from the EU e.g. to remove references to cross-border data transfers with other Member States and participation in EU wide-institutions such as the EDPB. See 'Keeling Schedule' for the UK GDPR, which shows the amendments
- Cross-border business must comply with both
- Legacy data (collected before 1/1/21) subject to 'frozen GDPR'

Essential elements in a data protection claim

Under Practice Direction 53B, para. 9, in any claim for breach of any data protection legislation the claimant must specify in the particulars of claim:

(1) the legislation and the **provision** that the claimant alleges the defendant has breached;

(2) any specific **data or acts of processing** to which the claim relates;

(3) the specific **acts or omissions** said to amount to such a breach, and the claimant's **grounds** for that allegation; and

(4) the **remedies** which the claimant seeks

Extraterritorial application

- *Soriano v Forensic News LLC* [2021] EWHC 56 (QB) – A US website (D) alleged that the claimant (C) was the "thug" of the Israeli Prime Minister, that he had corrupt links to Russia, and that he was involved in money laundering and illegal activity. Can the court examine this claim under any of the three criteria for the extraterritorial application of the GDPR, arts 3(1), 3(2) and 79(2)?
  - **Establishment** – D did not have any **stable arrangements** in the UK: no employees or representatives in the UK; a “handful” of UK subscriptions not sufficient
  - **Offer of goods or services** – D did not directly target UK consumers with its goods and services; UK shipping destination for the website’s merchandise but lack of actual purchases (only a baseball cap)
  - **Monitoring** of behaviour of EU residents – D used cookies for the purpose of behavioral profiling or monitoring in the context of targeted advertising, not to propagate the news (activity unrelated to the C’s claim)

Misuse of private information (Soriano continued)

- Misuse of private information - The claimant had a real prospect of establishing a breach of ECHR art 8 in respect of the photographs taken from open social media accounts. Even if "sourced from the public domain" [110], information which is technically available to the public online can still be information in which an individual enjoys a reasonable expectation of privacy against mass dissemination (*Green Corns Ltd v Claverley Group Ltd* [2005] EWHC 958 (QB) and the photos "do depict the Claimant in a private or personal setting, along with family members" [110]. Plus, article 8 extends to the right to reputation if the infringement is sufficiently serious (*Yeo v Times Newspapers* [2015] EWHC 2853 (QB)
- "That the Claimant has a real prospect of success in establishing a breach of his article 8 rights is insufficient…the court retains a discretion in service-out cases…needs to succeed on his libel claim" [111]: succeeded in relation to it as he was a British citizen and his personal and business life, as well as his reputation, were centred within the jurisdiction

Right of access

- *Lees v Lloyds Bank Plc* [2020] EWHC 2249 (Ch)
- Between 2010 and 2015 Lloyds and Mr Lees, the data subject, entered into buy-to-let mortgages with respect to three properties which in 2019 became subject to orders for possession. Lloyd responded to some but not all DSARs
- Chief Master Marsh stated even if Lloyds failed to respond to DSARs, the court would not exercise its discretion as to whether or not to issue an order to make Lloyds comply
  - The numerous and repetitive DSARs were abusive
  - The real purpose of the DSAR was to obtain the documents rather than personal data
  - Collateral purpose behind the requests was to obtain assistance in preventing Lloyds bringing claims for possession
  - Data sought would be of no benefit to Mr Lees

Data retention

- *R (on the application of II) v Commissioner of Police of the Metropolis* [2020] EWHC 2528 (Admin) – in 2015, under the UK Gov "Prevent Strategy" an 11-year old student was referred to the Counter Terrorism Commond of the Met due to radicalisation risk (he liked the television series Game of Thrones because of the beheadings). In 2016 the case was closed but data retained on ten databases accessible by police officers, counter terrorism officers, local authorities and the Home Office
- Now 16, C submitted that retention of the data breached ECHR art 8 and the first, third and fifth data protection principles of transparency/lawfulness/fairness, data minimisation, and storage limitation (DPA, ss 35, 37, 39 about LEA processing) → judicial review of the D's decision to retain his personal data and refusing the requests of his mother for such material to be deleted

Data retention (continued)

- The High Court granted the application:
  - Case was closed in 2015 **on its merits** because it was assessed that there was no cause for concern + nearly **5 years** passed + D underestimated the **impact of the interference** with the claimant's privacy rights (e.g. fear data disclosed to unis) → continued retention of C's personal data disproportionate and unjustified interference with art 8 ECHR (*R. (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9 followed)
  - Common ground that **the outcome of the proportionality assessment under art 8 ECHR should provide the answer** to whether continued retention was "necessary" under the DPA
    - For the reasons given in relation to art.8, continued retention of the claimant's personal data was disproportionate, was not necessary and so would breach the first and fifth data protection principles [85-88]

Data exports

Transfers of personal data from EU to 3rd countries

Adequacy Decision

Partial/Sectoral adequacy decision

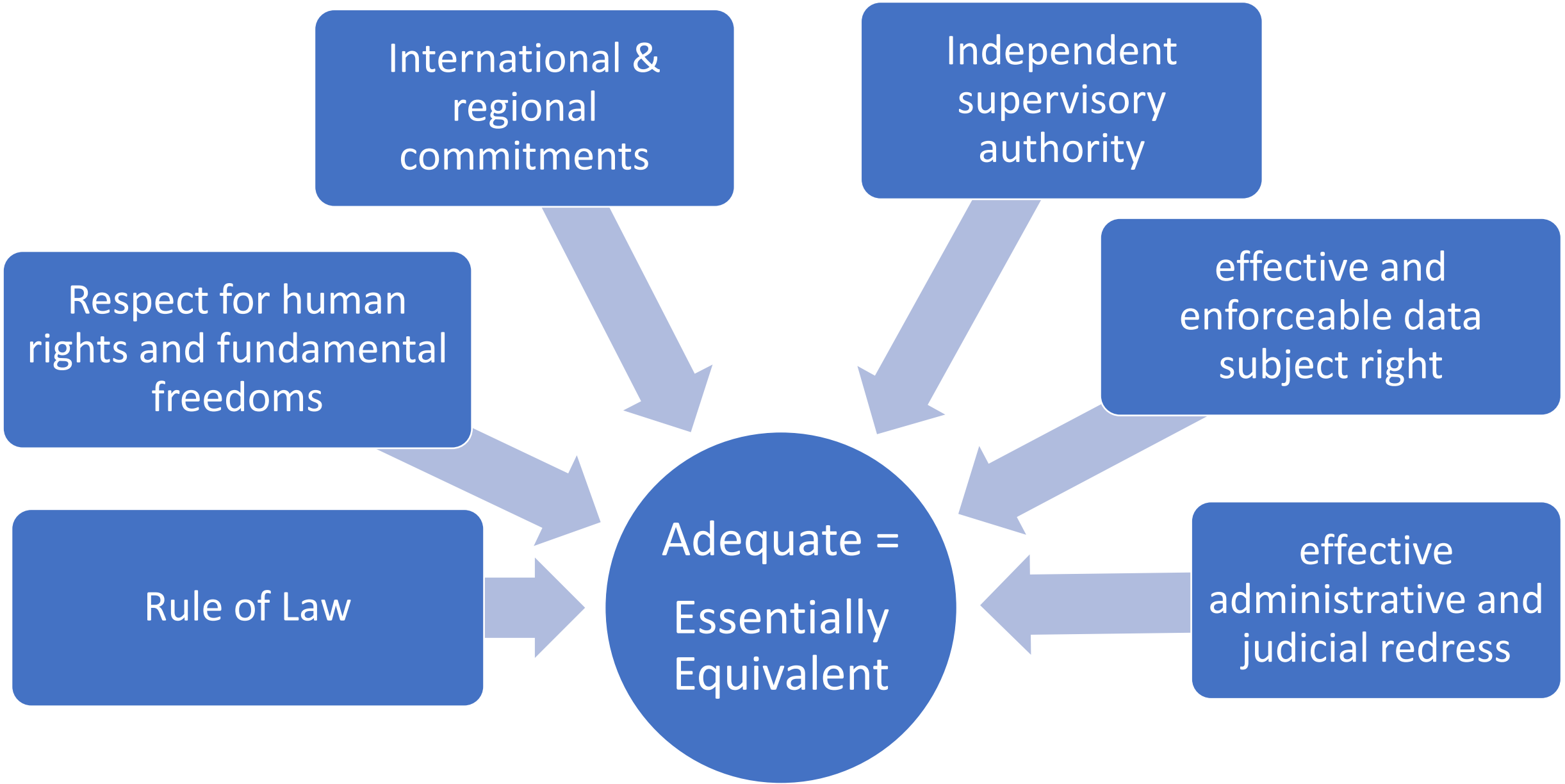
Binding Corporate Rules

Standard Contractual Clauses

Approved Codes of Conduct/Certification

Derogations esp. Consent

Art 45, GDPR


International & regional commitments
Independent supervisory authority
Respect for human rights and fundamental freedoms
effective and enforceable data subject right
Rule of Law
Adequate = Essentially Equivalent
effective administrative and judicial redress

13 Adequacy decisions (prior to July 2020)

The European Commission had issued adequacy decisions for the following countries:

- Andorra, Argentina, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The Commission had issued *partial adequacy* decisions for

- **Canada** and the **United States of America** (commercial organisations)
- In July 2020, US decision (Privacy Shield) invalidated by CJEU in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems,* ECLI:EU:C:2020:559
- In June 2021, draft decision on the adequacy of the Republic of Korea (thumbs up by EDPB in September 2021) and….

Transfers from the EEA into the UK

- In June 2021, the Commission adopted two adequacy decisions for the UK - one under the General Data Protection Regulation (GDPR) and the other for the Law Enforcement Directive
- UK data protection laws provide “essentially equivalent level of protection” to that guaranteed under EU law
- The decisions facilitate the correct implementation of the EU-UK Trade and Cooperation Agreement (TCA), which includes a commitment by the EU and UK to uphold high levels of data protection standards and foresees the exchange of personal information e.g. for cooperation on judicial matters
- Strong safeguards in case of future divergence such as a ‘sunset clause’, which limits the duration of adequacy to four years
- For more information read the adequacy decisions and related documents

Key elements of the adequacy decisions

- Essentially equivalent because UK GDPR ≈ EU GDPR + subject to ECtHR jurisdiction + abides by ECHR and Convention 108
- With respect to access to personal data by public authorities in the UK for national security reasons, the UK system provides for strong safeguards e.g. collection of data by intelligence authorities is subject to prior authorisation by an independent judicial body and unlawful surveillance may be actioned before the Investigatory Powers Tribunal
- During the four years of the sunset clause, the Commission monitors the legal situation in the UK and could intervene at any point
- Transfers for the purposes of UK immigration control are excluded from the scope of the adequacy decision

International data transfers from the UK

- Transitional arrangements under the TCA:
  - We can still use the Commission's adequacy decision to transfer data to EEA
    - UK government has the power to make its own 'adequacy regulations'
  - Continued use of EU Standard Contractual Clauses ('SCCs'), valid as at 31 December 2020, both for existing restricted transfers and for new restricted transfers
    - In June 2021, Commission adopted new SCCs (but after Brexit…)
  - Certain Binding Corporate Rules transition into the UK regime
- The UK GDPR restricts transfers of personal data outside the UK unless the rights of the individuals in respect of their personal data are protected in another way, or one of a limited number of exceptions applies
- A transfer of personal data outside the protection of the UK GDPR (which we refer to as a '**restricted transfer**'), most often involves a transfer from the UK to another country

Key questions for UK data exporters

1) Are we making a restricted transfer?

2) Are the restricted transfers legal?

2.1. Do we need to make a restricted transfer of personal data in order to meet our purposes?

Make transfer without personal data, otherwise go to 2.2

2.2. Are there UK ‘adequacy regulations’ in relation to the country or territory where the receiver is located or a sector which covers the receiver

If not, go to 2.3

2.3. Are we putting in place one of the ‘appropriate safeguards’ referred to in the UK GDPR?

If yes go to 2.4, otherwise go to 2.5

2.4. DPIA confirms essentially equivalent protection?

If not go to 2.5

2.5. Does an exception apply?

If not, you cannot transfer the data

Are you making a ‘restricted tranfer’?

You are making a restricted transfer if:

- the UK GDPR applies to your processing of the personal data you are transferring (UK GDPR, art 2; DPA, s 207)
- you are sending personal data, or making it accessible, to a receiver to which the UK GDPR will not apply in relation to their processing of the data
- the receiver is legally distinct from you as it is a separate company, organisation or individual (incl. same corporate group, excl. employee)

Do we need to make a restricted transfer?

- Before making a restricted transfer you should consider whether you can achieve your aims without actually sending personal data.
- If you make the data anonymous so that it is never possible to identify individuals (even when combined with other information which is available to receiver), it is not personal data.

Is the country covered by an adequacy regulation?

- EU or EEA institutions, bodies, offices or agencies
- Same ‘third countries’ recognised by the EU
- Except the Republic of Korea, as after the end of the transition period

Is the restricted transfer covered by appropriate safeguards?

- If no adequacy regulation, ‘appropriate safeguard’ - ensure that both data exporter and the receiver are legally required to protect individuals’ rights and freedoms in respect of their personal data
- Before you may rely on an appropriate safeguard to make a restricted transfer, you must undertake a risk assessment to be satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.
  - This takes into account the protections contained in the ‘appropriate safeguard’ + the legal framework of the destination country (including laws governing public authority access to the data).
- If your assessment is that the appropriate safeguard does not provide the required level of protection, you may include additional measures (see EDPB rec. on supplementary measures)

Supplementary measures

- Technical measures e.g. strong encryption, pseudonymisation, split processing
  - Needed where the law of the foreign country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR transfer tools incl. impinging on the contractual guarantee of an essentially equivalent level of protection against access by the public authorities
- Additional contractual measures e.g. to use specific tech measures, transparency (e.g. on LEA requests), to take specific actions (e.g. challenge the LEA request)
  - Not capable of binding the authorities of that third country when they are not party to the contract, these measures may often need to be combined with other technical and organisational measures
- Organisational measures i.e. internal policies (need-to-know), organisational methods, and standards

Appropriate safeguards (arts 46-47)

- Binding Corporate Rules (BCRs)
  - Approved by ICO, intended for use by multinational corporate groups, groups of undertakings or a group of enterprises engaged in a joint economic activity such as franchises, joint ventures or professional partnerships
- Standard contractual clauses (SCCs)
  - contract data exporter/importer incorporates standard data protection clauses recognised or issued in accordance with the UK data protection regime. EU SCCs are still valid (even though *Schrems II* cast shadow on them). See controller to controller; controller to processor
- Bespoke contractual clauses authorized by ICO
- A legally binding and enforceable instrument between public authorities or bodies (incl. int'l orgs)
  - Include enforceable rights and effective remedies for the individuals
- Administrative arrangements between public authorities or bodies
  - MoU authorized by ICO + effective and enforceable rights
- Approved code of conduct & certification – none so far
  - In May 2021, EDPB approved the first codes of conduct, presented by the Belgian and French but apply only to intra-EU processing and aim to provide practical guidance and define specific requirements for processors in the EU (GDPR, arts 40-41)

Is the restricted transfer covered by an exception? (art 49)

- If you are making a restricted transfer that is not covered by UK 'adequacy regulations', nor an appropriate safeguard, then you can only make that transfer if it is covered by one of the 'exceptions' set out in Article 49 ('true' exceptions to the rule)
- Explicit, specific (not restricted transfers in general), informed (incl. risks), easy to withdraw **consent**
- Necessary to perform a contract or to take steps requested by individual in order to enter into a **contract**
  - Occasional (more than once but not regularly) + can't perform the core purpose without it
- Necessary to enter into or perform a **contract that benefits another** individual whose data is being transferred
- Important reasons of **public interest**
  - Law allows transfer explicitly or impliedly e.g. International Convention for the Suppression of Acts of Nuclear Terrorism
- To establish if you have / make / defend a **legal claim**
  - **Occasional +** basis in law, and a formal legally defined process, but it is not just judicial or administrative procedures e.g. out-of-court procedures
- **Vital interests** of an individual lacking capacity to consent
- Transfer from a **public register** created under UK law (not whole categories of data)
- **One-off** and compelling **legitimate interest** (last resort)

Is the restricted transfer legal?

1. Adequacy decisions (now ‘adequacy regulations’)
2. Appropriate safeguards + ‘Transfer Impact Assessment (risk assessment that the level of protection would be essentially equivalent to UK data protection regime)
    1. *A legally binding and enforceable instrument between public authorities or bodies*
    2. *UK Binding corporate rules (“UK BCRs”)*
    3. *Standard contractual clauses (SCCs)*
    4. *An approved code of conduct*
    5. *Certification under an approved certification scheme*
    6. *Contractual clauses authorised by the ICO*
    7. *Administrative arrangements between public authorities or bodies*
3. Exceptions
    1. *Explicit consent*
    2. *Necessary to perform a contract or to take steps requested by individual to enter into a contract*
    3. *A contract with an individual which benefits another individual whose data is being transferred*
    4. *Public interest*
    5. *Legal claim*
    6. *Vital interest of the individual*
    7. *From public register*
    8. *One-off + compelling legitimate interest*

Sources

- Bailii: https://www.bailii.org/
- Information Commissioner's Office – Guides to legislation https://ico.org.uk/for-organisations/
- GDPR Hub: https://gdprhub.eu/index.php?title=Category:United_Kingdom
- WestLaw esp. "overview"
- Practical Law
- SSRN, ResearchGate, Academia.edu, Arxiv Law, Google Scholar, Google Books