



Data transfers to countries outside the EU/EEA under the GDPR

1 June 2017

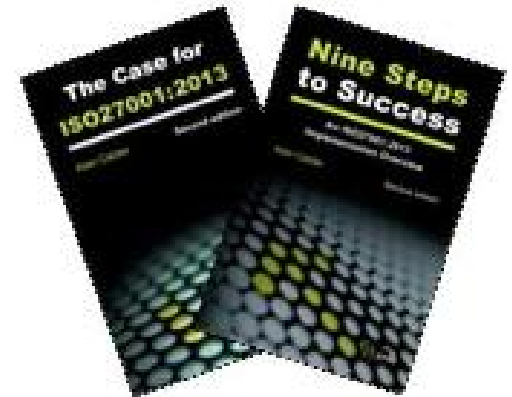
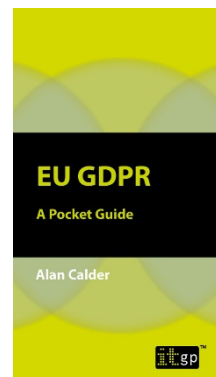
Alan Calder
Founder and Executive Chairman
IT Governance Ltd
www.itgovernance.co.uk

PLEASE NOTE THAT ALL DELEGATES IN THE WEBINAR ARE MUTED ON JOINING

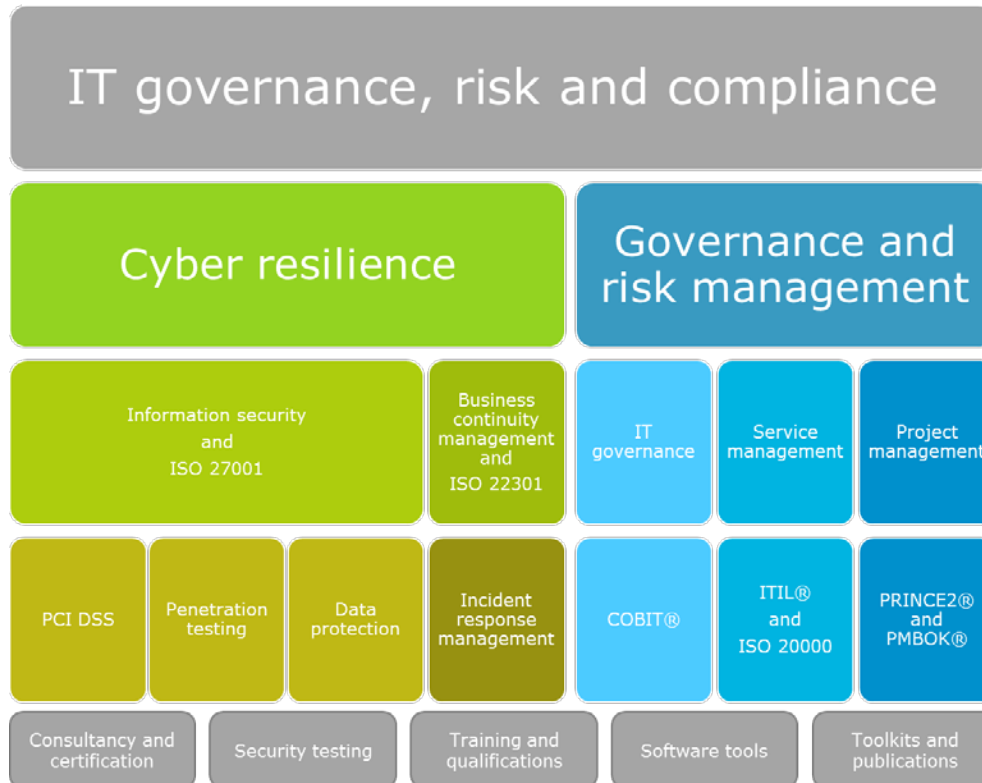
Introduction



- Alan Calder
- Founder – IT Governance Ltd
- The single source for everything to do with IT governance, cyber risk management and IT compliance
- IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 6th Edition (Open University textbook)
- www.itgovernance.co.uk



IT Governance Ltd: GRC One-stop shop



All verticals, all sectors, all organisational sizes

Agenda



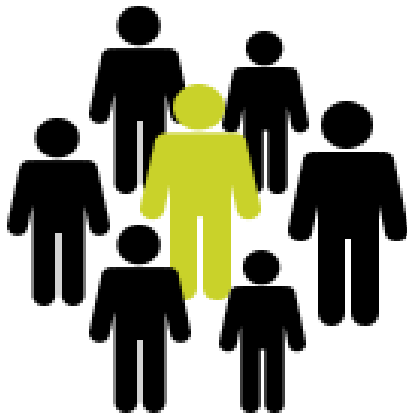
- A brief overview of the Regulation and its impact
- The rights of data subjects under GDPR
- The international transfer of data and appropriate safeguards.
- The derogations from general prohibition of data transfers outside the European Union.
- The requirements that govern one -off and infrequent transfers of personal data.
- The role of the supervisory authority in international transfers.

Articles 1 – 3: Who, and where?



Natural person = a living individual

- **Natural persons have rights associated with:**
 - The protection of personal data
 - The protection of the processing personal data
 - The unrestricted movement of personal data within the EU



- **In material scope:**
 - Personal data that is processed wholly or partly by automated means;
 - Personal data that is part of a filing system, or intended to be.
 - The Regulation applies to controllers and processors in the EU irrespective of where processing takes place.

The GDPR applies to controllers not in the EU

Remedies and liabilities



Natural Persons have rights

- Judicial remedy where their rights have been infringed as a result of the processing of personal data.
 - In the courts of the Member State where the controller or processor has an establishment.
 - In the courts of the Member State where the data subject habitually resides.

- Any person who has suffered material, or non-material, damage shall have the right to receive compensation from the controller or processor.

- Controller involved in processing shall be liable for damage caused by processing.



Penalties



Administrative fines



- In each case will be effective, proportionate, and dissuasive
 - taking into account technical and organisational measures implemented;
- **€10,000,000** or, in the case of an undertaking, up to **2%** of the total worldwide annual turnover of the preceding financial year.
- **€20,000,000** or, in case of an undertaking, **4%** total worldwide annual turnover in the preceding financial year.

Entry into force and application



“This Regulation shall be binding in its entirety and directly applicable in all Member States.”

KEY DATES

- On 8 April 2016, the European Council adopted the Regulation.
- On 14 April 2016, the European Parliament adopted the Regulation
- On 4 May 2016, the official text of the Regulation was published in the EU Official Journal in all the official languages.
- The Regulation entered into force on 24 May 2016, and will apply from 25 May 2018.
- http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Final text of the Regulation: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679>

Personal Data Breaches



Definition:

- A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Obligations

Data processor



- Notify data controller without delay
- No exemptions
- All data breaches have to be reported
- European Data Protection Board (EDPB) to issue clarification with regard to 'undue delay'



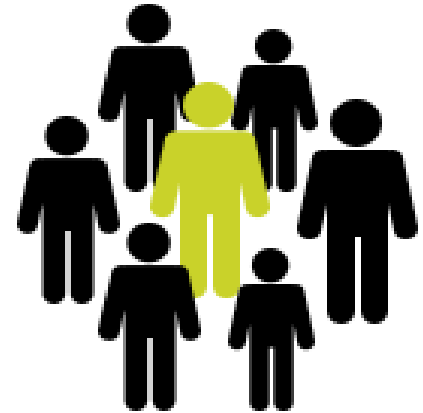
Data controller

- Notify supervisory authority no later than 72 hours
- Unnecessary in certain circumstances
- Description of the nature of the breach
- No requirement to notify if no risk to rights and freedoms of natural persons
- Failure to report within 72 hours requires explanation

Rights of Data Subjects



- The controller shall take appropriate measures to provide any information ... relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 11-1)
- The controller shall facilitate the exercise of data subject rights (Article 11-2)
 - Rights to
 - Consent
 - Access
 - Rectification
 - Erasure
 - Restriction
 - Objection
 - the right to data portability;
 - the right to withdraw consent at any time;
 - the right to lodge a complaint with a supervisory authority;
 - The right to be informed of the existence of automated decisionmaking, including profiling, as well as the anticipated consequences for the data subject.



Principles...from 8 to 6



1 • Lawfulness, fairness & transparency

2 • Purpose limitation

3 • Data minimisation

4 • Accuracy

5 • Storage limitation

6 • Rights – no longer a principle

7 • Integrity & confidentiality

8 • Transfers – no longer a principle

Personal data, international organisations, non-EEA states and the EU-US Privacy Shield



Transfer of personal data to third countries or international organisations



Article 44: General principle for transfers

- Any transfer of personal data by controller or processor shall take place only if certain conditions are complied with:
 - a. Transfers on the basis of adequacy;
 - b. Transfers subject to the appropriate safeguards
 - c. Binding corporate rules apply.
- All provisions shall be applied to ensure the protection of natural persons is not undermined.

Transfer of personal data to third countries or international organisations

Recitals 103-107, 169, Article 45



a) Transfers on the basis of adequacy

- A transfer may take place where there is an adequate level of protection.
- The adequacy criteria:
 - the rule of law;
 - respect for human rights and fundamental freedoms;
 - relevant legislation, both general and sectoral, including:
 - concerning public security;
 - defence;
 - national security; and
 - criminal law.
- *Official Journal of the European Union (published on the EU Commission website)*

Transfer of personal data to third countries or international organisations

Recitals 103-107, 169, Article 45



a) Transfers on the basis of adequacy

No restrictions on transfers to EEA Countries

Austria

Belgium

Bulgaria

Croatia

Cyprus

Czech Republic

Denmark

Estonia

Finland

France

Germany

Greece

Hungary

Iceland

Ireland

Italy

Latvia

Liechtenstein

Lithuania

Luxembourg

Malta

Netherlands

Norway

Poland

Portugal

Romania

Slovakia

Slovenia

Spain

Sweden

United Kingdom

Transfer of personal data to third countries or international organisations



Recitals 103-107, 169, Article 45

a) Transfers on the basis of adequacy

The following additional countries are considered by the EU as having adequate data protection laws:

Andorra

Argentina

Canada

Faroe Islands

Guernsey

Isle of Man

Israel

Jersey

New Zealand

Switzerland

Uruguay

Transfer of personal data to third countries or international organisations



a) Transfers on the basis of adequacy

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

- Authorisations of transfers made by member states or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.



Transfers of personal data to third countries or international organisations



Recital 108-10, 114, Article 46

b) Transfers subject to appropriate safeguards

Adequate safeguards include:

- a legally binding agreement between public authorities or bodies;
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted in to administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Transfer of personal data to third countries or international organisations



Recitals 111, 112, Article 49

Derogations

GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations.

Conditions on when a derogation applies:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

Transfer of personal data to third countries or international organisations

Recitals 113, Article 49



What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

One-off transfers are permitted only where the transfer:

- cannot be made on the basis of an adequacy finding, or standard contract clauses, or binding corporate rules, or one of the derogations,
- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual)
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations must inform the relevant supervisory authority of the transfer and inform the data subject of the compelling legitimate interests pursued.

Model contract clauses as a basis for transferring personal data outside the EEA



The European Commission is empowered to recognise standard contractual clauses (known as model contract clauses) as offering adequate safeguards for the purposes of Article 26(2)1.

- Current model contract clauses apply to DPD
 - http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm
- Two sets for controller – controller transfers
 - Set II considered more ‘business-friendly’
- One set for controller – processor transfers
- FAQs on use of model contract clauses
 - http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf

Model contract clauses as a basis for transferring personal data outside the EEA



Amending the clauses, incorporating the clauses in other contracts and inserting additional clauses

- If you are relying on any of the European Commission sets of model contract clauses as 'stand-alone contracts' you cannot change the clauses in any way (other than to add an additional party, such as an additional data importer).
- The model contract clauses may be incorporated into other contracts (such as data processing service agreements) provided nothing in the other contract or additional clauses alters the effect of any of the model clauses.

Model contract clauses as a basis for transferring personal data outside the EEA



Drawbacks with the use of contracts

- Potentially hundreds of contracts are required to cover transfers between all entities.
- Burden to ensure contracts are kept up -to-date to keep pace with the changing corporate structure can be difficult and time consuming.

Binding corporate rules



What are Binding Corporate Rules designed to achieve?

- Binding Corporate Rules (BCRs) are designed to allow multinational companies to transfer personal data from the European Economic Area (EEA) to their affiliates located outside of the EEA.
- Applicants must demonstrate that their BCRs put in place adequate safeguards for protecting personal data throughout the organisation.
- Existing model BCRs are DPD -related

Binding corporate rules



How to get authorisation for BCRs?

- You need to choose a supervisory authority to be a lead authority.
 - Complex application process
 - Standard application form, BCR checklist
 - <https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/>
- If the lead authority is satisfied as to the adequacy of the safeguards put in place in your BCRs, that authority decision is binding across the other supervisory authorities in Europe
 - Other member states may have additional requirements

It is important to note that BCRs do not provide a basis for transfers made outside the group, nor do they work for a single international entity.

Binding corporate rules



What are the benefits of BCRs?

- BCRs can provide a framework for intragroup transfers.
- Ongoing obligation to monitor your compliance
 - regular audits
 - maintain a training programme for staff handling personal data.

Any change to process requires a reapplication

Privacy Shield

Applies to transfers to US only



- The decision on the EU -U.S. [Privacy Shield](#) was adopted by the European Commission on 12 July, 2016

Commercial sector

Strong obligations on companies and robust enforcement

U.S Government access

Clear safeguards and transparency obligations

Redress

Directly with the company
With the data protection authority
Privacy shield panel

Monitoring

Annual joint review mechanism between US Department of commerce and EU Commission

Privacy Shield

Applies to transfers to US only



Why should an organisation that previously participated in the Safe Harbor program self-certify to the Privacy Shield?

- The Privacy Shield Framework was deemed adequate by the European Commission.
- Participating organisations are deemed to provide “adequate” privacy protection,
- Compliance requirements of the Privacy Shield Framework are clearly laid out and can be implemented by small and medium-sized enterprises.




Privacy Shield

Applies to transfers to US only



The information that an organisation must provide during the self-certification process includes:

- Company name
 - Address
 - Contact
 - Mechanism to investigate complaints
 - Description of privacy policy
- 
- An illustration of a laptop computer. On the screen, there is a large, yellow-green icon of an open padlock, symbolizing security or access.
- The following URL must be included in an organisation's privacy policy to meet the Framework requirement <https://www.privacyshield.gov>

Privacy Shield Principles



1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement and Liability



Apps & Cloud Services



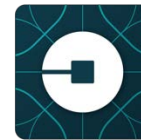
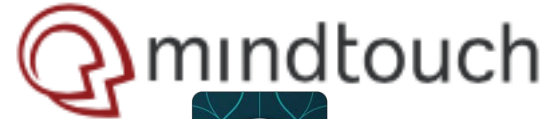
RFP Responses Made Simple.



WhatsApp



GitHub



GDPR: Controllers or processors outside the EU



Article 27: Representatives of controllers or processors not established in the Union

- Recital 23: In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.
- Where the controller or the processor are not established in the Union:
 - They shall designate in writing a representative in the Union;
 - Representative shall be established where data processing or profiling resides;
 - The representative shall be mandated to be addressed by supervisory authorities and data subjects for the purposes of the Regulation;
 - Designation of representative does not absolve controller or processor from legal liabilities.

GDPR: Cloud processor obligations

Policy and procedure requirements



Article 28: Processor

A legal contract must ensure that the processor:

- processes the personal data only on documented instructions from the controller;
- ensures that persons authorised to process the personal data observe confidentiality;
- takes appropriate security measures;
- respects the conditions for engaging another processor;
- assists the controller by appropriate technical and organisational measures;
- assists the controller in ensuring compliance with the obligations to security of processing;
- deletes or returns all the personal data to the controller after the end of the provision of services;
- makes available to the controller all information necessary to demonstrate compliance with the Regulation.

International transfers & Cloud providers



- The Cloud is not automatically territorially limited
- Any transfer of personal data by controller or processor shall take place only if certain conditions are complied with:
 - Transfers on the basis of adequacy;
 - Transfers subject to the appropriate safeguards
 - Binding corporate rules apply.
- All provisions shall be applied to ensure the protection of natural persons is not undermined.
- To countries with similar data protection regulations
 - Cloud providers are a key risk area
 - Highest penalties apply to breaches of these provisions
- Cloud providers need to ensure they are able to differentiate their EU and non-EU provision and provide clarity to data subjects and controllers



Cloud-based services



- Controller still needs legitimizing reason for transfer;
- Data protection principles still apply;
- Use of model clauses meets the above requirement;
- Obligation is on the data controller to ensure compliance with law;
- Obligation on the data controller to inform data subjects of transfer.

IT Governance: GDPR Consultancy



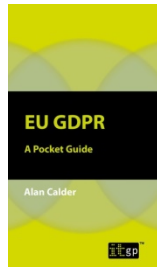
- **Gap analysis**
- Our experienced data protection consultants can assess the exact standing of your current legal situation, security practices and operating procedures in relation to the DPA or the GDPR.
- **Data flow audit**
- Data mapping involves plotting out all of the organisations' data flows, which involves drawing up an extensive inventory of the data to understand where the data flows from, within and to. This type of analysis is a key requirement of the GDPR.
- **Information Commissioner notification support (a legal requirement for DPA compliance)**
- Organisations that process personal data must complete a notification with the Information Commissioner under the DPA.
- **Implementing a personal information management system (PIMS)**
- Establishing a PIMS as part of your overall business management system will ensure that data protection management is placed within a robust framework, which will be looked upon favourably by the regulator when it comes to DPA compliance.
- **Implementing an ISMS compliant with ISO 27001**
- We offer flexible and cost-effective consultancy packages, and a comprehensive range of bespoke ISO 27001 consultancy services, that will help you implement an ISO 27001-compliant ISMS quickly and without the hassle, no matter where your business is located.
- **Cyber health check**
- The two -day Cyber Health Check combines on-site consultancy and audit with remote vulnerability assessments to assess your cyber risk exposure.

www.itgovernance.co.uk/dpa-compliance-consultancy

IT Governance: GDPR one-stop shop

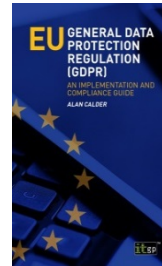


Self-help materials



A Pocket Guide

www.itgovernance.co.uk/shop/Product/eu-gdpr-a-pocket-guide



Implementation manual

www.itgovernance.co.uk/shop/Product/eu-general-data-protection-regulation-gdpr-an-implementation-and-compliance-guide



Documentation Toolkit

www.itgovernance.co.uk/shop/Product/eu-general-data-protection-regulation-gdpr-documentation-toolkit



Compliance Gap Assessment Tool

www.itgovernance.co.uk/shop/Product/eu-gdpr-compliance-gap-assessment-tool

IT Governance: GDPR one-stop shop



Training courses



1-Day accredited Foundation course (classroom, online, distance learning)

www.itgovernance.co.uk/shop/Product/certified-eu-general-data-protection-regulation-foundation-gdpr-training-course



4-Day accredited Practitioner course (classroom, online, distance learning)

www.itgovernance.co.uk/shop/Product/certified-eu-general-data-protection-regulation-practitioner-gdpr-training-course



1-Day Data Protection Impact Assessment (DPIA) Workshop (classroom)

www.itgovernance.co.uk/shop/Product/data-protection-impact-assessment-dpia-workshop

Questions