



Data Protection after Brexit – what you need to know

WITH PAUL TICHER



**Our mission is to help
London's small charities and
community groups unlock
the value of data**

www.datawise.london

DISCOVER. LEARN. ANALYSE. SHAPE. REPEAT

#DatawiseLondon





COALITION
— FOR EFFICIENCY —

Makerble

DataKindUK

hear
humanity. equality. rights.

london plus





Access resources and 1:1 support
via www.datwise.london

See training available [on our
Eventbrite page](#)

Sign up to our monthly eNews at
www.superhighways.org.uk/e-news



PAUL | TICHER

GDPR and Brexit

November 2020

PAUL | TICHER

This presentation is intended to help you understand aspects of the Data Protection Act 2018, the General Data Protection Regulation and related legislation.

It is not intended to provide detailed advice on specific points, and is not necessarily a full statement of the law.

What Data Protection is about: 1

Protecting
data



Protecting people



Clients Service users Beneficiaries
Employees Volunteers Trustees
Donors Members Customers
Supporters Professional contacts

- Keeping information in the right hands (and knowing what the 'right hands' are)
- Holding good quality data

What Data Protection is about: 2



Transparency & choice

What Data Protection is about: 3

- * Recognise individual rights, such as:

- * Right of Subject Access



- * Right to opt out of direct marketing



- * ... and now many others

Elements of GDPR



Compliance

Lawful basis

Principles

Data Controller

Processing

Personal data

(Data) Controller (Article 4(7))

“'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;”

Joint controllers (Article 26)

“Where two or more controllers jointly determine the purposes and means of processing, they shall be **joint controllers**. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information ...”

Data Processors

- * Organisation (or possibly sole trader) that processes data on your behalf
- * Must have a contract
- * Contract must meet the requirements of GDPR
- * Processors can be directly liable if they disobey you
- * A cloud provider, for example, would most likely be a processor

Lawful basis for processing (Art 6)

At least one of the following:

- * With consent of the Data Subject
- * For a contract involving the Data Subject
- * To meet a legal obligation
- * To protect any person's 'vital interests'
- * Government & judicial functions
- * In your 'legitimate interests' provided the Data Subject's interests are respected

Where
necessary

Consent

Consent is “any freely given, specific, informed and **unambiguous** indication of his or her wishes by which the data subject, either by a statement or by a **clear affirmative action**, signifies agreement to personal data relating to them being processed” (Article 4(11))

“Silence, pre-ticked boxes or inactivity should ... not constitute consent.” (Recital 32)

Obtaining valid consent

- * “[A] request for consent must be presented in a manner which is clearly distinguishable from ... other matters, in an intelligible and easily accessible form, using clear and plain language.” (Article 7 (2))
- * “The data subject shall have the right to withdraw his or her consent at any time.” (Article 7 (3))
- * “When assessing whether consent is freely given, utmost account shall be taken of whether ... a contract ... is made conditional on [consent to processing] that is not necessary for the performance of this contract.” (Art 7 (4))

Record-keeping

- * Where processing is based on consent, the controller shall be able to **demonstrate** that the data subject has consented to processing of his or her personal data.
- * This means keeping some record of who gave consent, when, how and what for (and whether it has since been withdrawn).

The Data Protection Principles

- a) Data 'processing' must be 'fair' and legal
- b) You must limit your use of data to the purpose(s) you obtained it for
- c) Data must be adequate, relevant & **limited to what is necessary**
- d) Data must be accurate & up to date where necessary
- e) Data must not be held longer than necessary
- f) You must have appropriate security

First two Principles (Art 5(1)(a) & (b))

“Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');”
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- * This means, in particular, that people must know enough about what you want to do, or are doing, with their data, and in some detail

Transparency

Data Subjects must usually be made aware of (Article 13):

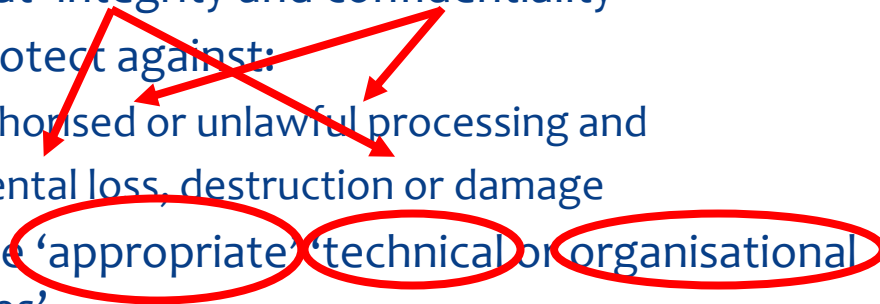
- * the identity and the contact details of the controller
- * the purposes as well as the legal basis of the processing
 - * where relevant the legitimate interests
 - * where relevant the right to withdraw consent at any time
- * any recipient(s); any overseas transfers
- * the storage period or criteria for deletion
- * right of access to data and rectification or erasure
- * any profiling or automated decisions, and right to object
- * right to lodge a complaint with the Information Commissioner
- * whether ... the data subject is obliged to provide the data and ... possible consequences of failure to provide [it]

The next three Principles (A5 (1)(c-e))

Data must be:

- * adequate, relevant and limited to what is necessary in relation to the purposes ... ('data minimisation')
- * accurate and, where necessary, kept up to date; every reasonable step must be taken to [erase or rectify] personal data that are inaccurate ... without delay ('accuracy')
- * kept in a form which permits identification of data subjects for no longer than is necessary ('storage limitation')

Sixth Principle (Article 5(1)(f))

- * Aiming at 'integrity and confidentiality'
 - * Must protect against:
 - * unauthorised or unlawful processing and
 - * accidental loss, destruction or damage
 - * Must use 'appropriate technical or organisational measures'
 - * 'Data minimisation' also helps
- 

What happens on 1st January?

- * UK no longer subject to GDPR, but to ‘UK GDPR’ – almost identical, but without references to EU institutions.
- * Other minor adjustments
- * Transfers to EU (and other countries) unaffected.
- * Transfers *from* EU less straightforward
- * Our rules may change: suggestions that the government’s National Data Strategy may lead to watering down.

Easy options for transfers abroad

- * Within the European Economic Area
 - * EU plus Norway, Iceland, Liechtenstein
- * EU (or UK) decision on adequacy
 - * Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay
 - * Gibraltar (UK only)
 - * Canada, Japan (partial)
 - * USA (see next slide)

Difficult areas

- * USA – Privacy Shield (but maybe not – July 2020 decision of the EU Court of Justice)
- * Standard contractual clauses (SCC) / binding corporate rules (BCR)
- * Specified situations
- * Other options

Specified situations where transfer is permitted

- * data subject informed consent;
- * necessary for the performance of a contract between the data subject and the controller;
- * necessary for the conclusion or performance of a contract in the interest of the data subject;
- * necessary for important reasons of public interest;
- * necessary in connection with legal claims;
- * necessary to protect the vital interests of the data subject or others, where the subject is incapable of giving consent;
- * transfer from a public register.

Also permitted

A transfers that:

- * is not repetitive;
- * concerns only a limited number of data subjects;
[and]
- * is necessary [in the controller's] compelling legitimate interests, which are not overridden by the interests, rights and freedoms of the data subject.

Scenario 1: Cloud provider

- * If based in EU:
 - * Data transfer from UK = no problem
 - * Data transfer from EU back to UK = until positive adequacy decision, should be based on SCC
- * If based overseas with adequacy decision:
 - * Data transfer from UK = no problem
 - * Data transfer back to UK = depends on their rules (SCC?)
- * If based overseas without adequacy decision:
 - * Data transfer from UK = must use SCC
 - * Data transfer back to UK = depends on their rules (SCC?)

Scenario 2: data subjects abroad

- * If based in EU:
 - * Data transfer from EU to UK = probably OK
 - * Data transfer from UK back to EU = no problem
- * If based overseas with adequacy decision:
 - * Data transfer to UK = depends on their rules (probably OK)
 - * Data transfer back from UK = no problem
- * If based overseas without adequacy decision:
 - * Data transfer to UK = probably OK
 - * Data transfer back from UK = probably OK

Fly in the ointment

- * Standard Contractual Clauses (in current form at least) are probably not sufficient for transfers to the USA
- * What to do?
 - * Nobody knows!

Upshot

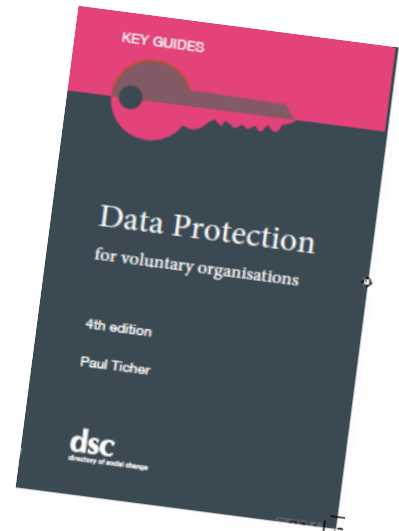
- * Make sure you know where your data is stored when using cloud providers
- * Explore how far the provider has got in incorporating SCCs into their contract
 - * -- with the exception of the USA, of course
- * Review any other *regular* transfers to ensure they are acceptable
- * Have a procedure for checking that occasional transfers are acceptable

Advert

Data Protection for Voluntary Organisations (4th edition)

Publication: January 2021

Publisher: Directory of Social Change



Thank you

Any questions:

paul@paulticher.com