11KBW

# The GDPR: Regulatory guidance so far

Robin Hopkins

robin.hopkins@11kbw.com

6 March 2019

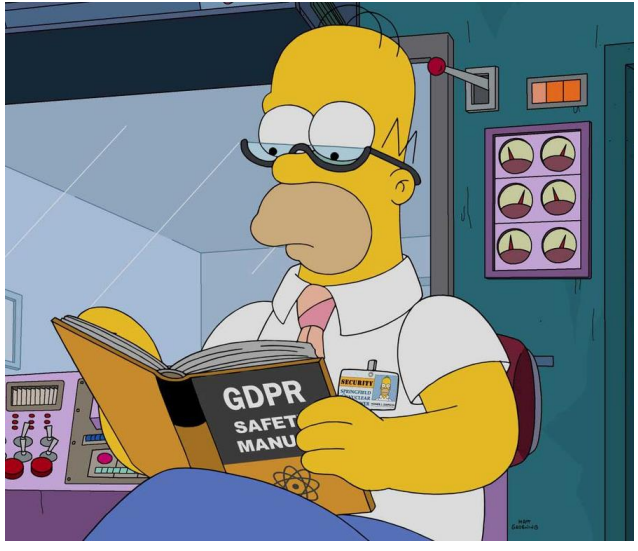
# GDPR: sources of guidance?

11KBW

Two main sources of regulatory guidance:

1. ICO's comprehensive guides to data protection and the GDPR*

2. EDPB topic-specific guidelines**




* https://ico.org.uk/for-organisations/guide-to-data-protection/whats-new/

** https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

# Territorial scope (1)

11KBW

Two main limbs – "establishment" and "monitoring"

- **Establishment – Art 3(1):**
  processing in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not

- **Targeting – Art 3(2):**
  processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  (b) the monitoring of their behaviour as far as their behaviour takes place within the Union

# Territorial scope (2)

11KBW

**EDPB Draft Guidelines 3/2018 (16 Nov 2018) – Art 3(1):**

Establishment:

- Substance not form: *"implies the effective and real exercise of activities through stable arrangements"* (Recital 22)
- Broad (can be minimal, e.g. via 1 employee) but not unlimited (website accessibility is insufficient); *in concreto* analysis

"In the context of the activities":

- Broad – look for "inextricable link" e.g. revenue-raising
- But some commercial activity within the EU may be *"so far removed from the processing of personal data"* that the GDPR does not apply

Consider controllers and processors separately:

- A processor will generally not be an "establishment" of a controller
- GDPR could apply to a processor but not to its controller

# Territorial scope (3)

**EDPB Draft Guidelines 3/2018 (16 Nov 2018) – Art 3(2):**

- Data subjects in the EU: physically in EU, not nationality/residence

- Offering goods or services:
  - Includes: online services; free services
  - Consider whether controller has "manifested its intention to establish commercial relations" with data subjects in the EU
  - Indicators: EU contact details, language, currency, delivery, web domain; nature of service; search engine use; clientele references

- Monitoring behaviour:
  - Consider intention to target and purposes of processing
  - Any online collection or analysis of personal data will suffice

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

# Lead supervisory authorities

11KBW

**A29 guidelines (wp244, revised April 2017):**

- LSA mechanism (Arts 55-56) applies to 'cross-border processing' (defined in Art 4(23)): processing in context of >1 EU establishment, or substantially affects data subjects in >1 EU state

- LSA for the cross-border processing will then be the supervisory authority of controller/processor's 'main establishment'. Usually central administration, but look for:
  - data processing decision-making/power (for controllers), or
  - where the main processing activities take place (for processors)

How to decide? Consider:

- Where are decisions re purposes and means of the processing given final 'sign off'?
- Where are decisions about business activities that involve data processing made?
- Where does power to have decisions implemented effectively lie?
- Where are directors with overall management responsibility for the cross-border processing based?
- Where is the controller/processor registered as a company?

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

# Definition of personal data

11KBW

**ICO detailed guidance (May 2018):**

Reiteration of key concepts, including:

- Hypothetical or ‘very slight’ identification risk insufficient
- Consider use-case, e.g. singling out

Helpful examples, including:

- HR department ‘anonymising’ job applications
- CCTV footage when identity not known
- Wi-fi and device-specific Media Access Control (MAC) addresses
- Market value of a house

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/

# Controllers & processors

11KBW

## ICO guidance (December 2018):

- Checklists for ‘am I controller, joint controller or processor?’

- Joint controller indicators (see Article 26 GDPR):
  - Common objectives regarding the processing
  - Processing for the same purpose as another controller
  - Using the same set of personal data (e.g. one database)
  - Designed this process with another controller
  - Common information management rules with another controller

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

# Consent (1)

11KBW

**Art 4(11) GDPR:**

- *“any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data”*

- See also Art 7: be able to demonstrate consent; use plain language; don’t bundle it in; make clear consent can be withdrawn

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/

# Consent (2)

11KBW

**ICO detailed guidance (May 2018):**

- Don’t use pre-ticked boxes/opt-outs/consent by default
- Specify identity of data controller, processing purposes, types of activity, right to withdraw consent
- Be ‘specific & granular’ but also ‘clear & concise’
- Update, especially if processing changes: no evolution!
- Explicit consent not much different
- If you can’t offer genuine choice, don’t rely on consent
- Consent may be difficult for employers & public authorities

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/

# Consent (3)

11KBW

**A29 WP guidance (wp259; July 2018):**

Freely given:

- Not bundled up with non-negotiable terms
- No detriment – at time of entry or when withdrawing consent
- Beware imbalances of power
- Interaction with performance of contract? Interpret that ground strictly

Specific:

- Granular, by purpose e.g. a controller suggesting preferences is different from third-party targeted advertising

# Consent (4)

11KBW

Informed:

- About the controller, purposes, profiling, withdrawal right, type of data, international transfers
- Plain language
- Highlight, separate – don't bury

Unambiguous positive action:

- Not just words, could be e.g. swiping or turning up to an event

Have a refreshment strategy

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

# Other lawful processing conditions

11KBW

**Nuggets from ICO guidance:**

- Necessary for contract performance is not the same as 'necessary for my business'
- Legal obligation: *"does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute"*
- Public task: need not be statutory, but note legal certainty requirement
- *"Legitimate interests that are relevant are no longer limited to your own interests or those of third parties to whom you disclose the data. You can now consider the interests of any third party, including the wider benefits to society"*
- Best practice to conduct a LIA – see ICO template

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

# Transparency

11KBW

**A29 WP guidance (wp260; April 2018):**

- Transparent about what? Controllers, data, purposes, recipients, consequences, rights
- Concise, easily intelligible language
- Don’t use vague and broad language or ‘may’
- Easily accessible – no need to hunt for it
  - Never more than 2 taps away
  - Have tab on homepage
- Info must be “provided”, i.e. active steps to furnish, via appropriate means
  - Generally, this could be via a website privacy notice
  - But consider more active steps e.g. if substantial changes
- Layered approaches, push & pull notices, just-in-time transparency

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 See also https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/

# Data subjects' rights (1)

11KBW

**Main guidance: portability (Art 20) and automated decision-making (Art 22)**

**A29 guidelines on portability (wp242; April 2017):**

- Automated processing based on consent or contract necessity
- Right applies to data directly provided by data subject + data on observed activities (e.g. smart meter data, search history), but not data created/inferred/derived by the controller
- Must provide *"in a structured, commonly used and machine-readable format"*
- Also a right to transmit those data to another controller without hindrance
- Examples: move from webmail service to an archiving service; music streaming playlists; contact lists; smart meters; banking

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

- See also ICO guidance on exemptions

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

# Data subjects' rights (2)

**A29 guidelines on automated decision-making (wp251; August 2018):**

- Art 22(1): *"right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"*
- Distinguish profiling, decision-making partly using automated profiling and A22 solely automated decision-making (including profiling) that produces legal or similar effects
- Meaningful, rather than token human involvement
- Similar effects? online credit applications and e-recruiting; effects on financial position, access to health systems, employment opportunity, university admission
- Limited exceptions (contract, legal obligation, explicit consent)
- More stringency for special category data

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

# Records of processing activities

11KBW

**A29 'position paper' on Article 30(5) (April 2018):**

Duty to keep record of processing activities does not apply *"to an enterprise or an organisation employing fewer than 250 persons* unless:

- *(i) the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects,*
- *(ii) the processing is not occasional, or*
- *(iii) the processing includes special category/criminal data"*

To be exempt, must meet all three conditions

But if duty applies, the SME *"need only maintain records of processing activities for the types of processing mentioned by Article 30(5)"*

# Records of processing activities (cont.)

11KBW

What's the point again?

> *"… the record of processing activities is a very useful means to support an analysis of the implications of any processing whether existing or planned. The record facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security measures to safeguard personal data…"*

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045
On accountability and governance more broadly, see the ICO's guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

- /

# DP Impact Assessments (1)

KBW

**Art 35(1):** up-front DPIA requires *"where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons"*

**A29 guidelines (wp248; October 2017):**

What counts as high risk?

- Evaluation/scoring
- Automated profiling
- Systematic monitoring
- Non-obvious use of special category data
- Vulnerable data subjects
- Matching or combining datasets
- Processing on a large scale
- Using innovative technology
- Effect on data subjects, e.g. new bank loan/insurance applications

What should it look like? See Annex 2 to A29 Guidance

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
See also the ICO's guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

# DP Impact Assessments (2)

**More insights via EDPB's Opinion 22/2018 on ICO's draft list under Arts 35(5):**

- Processing of biometric/genetic/location data on its own is not necessarily likely to represent a high risk. *"However, the processing of such data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion [i.e. a risk indicator] requires a DPIA to be carried out"*.

- You don't necessarily need a DPIA when you rely on Art 14(5) (i.e. where you are declining to provide transparency info)

- You probably do need one whenever you are engaged in monitoring of employees

https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf

# Breach reporting

11KBW

**A29 guidance (wp250; August 2018) :**

- Art 33: must report to ICO within 72 hours of becoming aware unless the breach *"unlikely to result in a risk to the rights and freedoms of natural persons"*
- When do you "become aware"? When you have a reasonable degree of certainty that a breach has occurred
- When is a breach unlikely to result in a risk? Consider nature of data, whether you have a backup copy, and NB security protections (encryption, hashing, salting

Consider: type of breach; nature, sensitivity and volume of affected data; ease of identification of individuals; nature and severity of potential consequences for individuals; number of affected individuals

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

# Administrative fines

11KBW

## A29 guidelines on setting of administrative fines (wp253; Oct 2017)

- Equivalent protections and thus equivalent sanctions: *"it should be avoided that different corrective measures are chosen by the SAs in similar cases"*
- Fines should be *"effective, proportionate and dissuasive"*
- "Minor infringements" (Recital 148): in cases where infringement creates no significant risk & doesn't undermine essence of obligation, *"the fine may (but not always) be replaced by a reprimand"*
- Common-sense discussion of relevant considerations from Article 83: nature, gravity & duration of infringement; nature, scope or purpose of the processing; nature of data; number of data subjects affected; level of damage suffered; track record; degree of responsibility (see Arts 24, 25, 32); intentional/negligent; mitigating actions

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

# International transfers (1)

KBW

## ICO guidance (updated August 2018):

- What is a restricted transfer? The ICO's 3-step test:

  1. *"the GDPR applies to your processing of the personal data you are transferring"*

  2. *"you are sending personal data, or making it accessible, to a receiver to which the GDPR does not apply"*

  3. *"the receiver is a separate organisation or individual. This includes transfers to another company within the same corporate group. However, if you are sending personal data to someone employed by you or by your company, this is not a restricted transfer. The transfer restrictions only apply if you are sending personal data outside your organisation"*

- Transit is not transfer

- Making personal data available online is a transfer

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

# International transfers (2)

**EDPB guidelines 2/2018 on derogations under Article 49 GDPR (November 2018):**

Interpreted restrictively: exception should not become rule

The derogations:

**a. Explicit consent**: must be specific for the particular transfer/set of transfers + after having been informed of the possible risks of such transfers

**b. Contract with data subject:** note necessity test (travel agency: necessary transfer; centralised HR function outside EU: unnecessary transfer)

**c. Contract in data subject's interests**

**d. Important reasons of public interest:** mainly aimed at public authorities, including for reciprocity where cooperation mechanisms are in place

# International transfers (3)

11KBW

The derogations continued:

**e. Legal claims etc:** must have basis in law, though not confined to judicial or administrative proceedings; need *"a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position"*

**f. Vital interests:** medical emergency, but also e.g. housing eviction

**g. Extracts from publicly available registers**

**Art 49(1) subpara 2 – compelling legitimate interests:** last resort; limited number of data subjects, not repetitive, balance competing interests, be transparent and implement safeguards

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

# All clear then?

11KBW