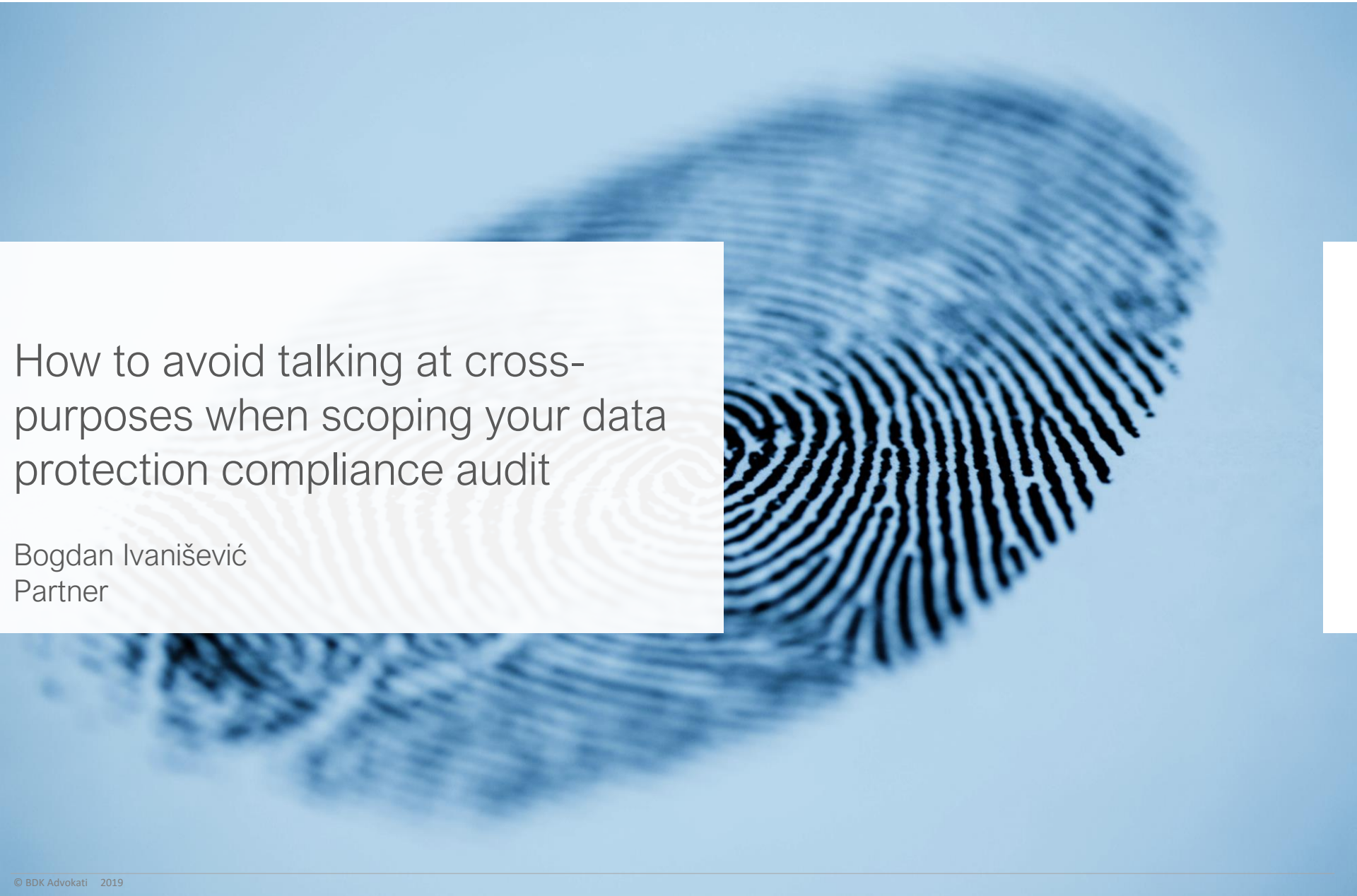
BDK Advokati



# How to avoid talking at cross-purposes when scoping your data protection compliance audit

Bogdan Ivanišević
Partner

BDK Advokati

# Table of content

BDK Advokati

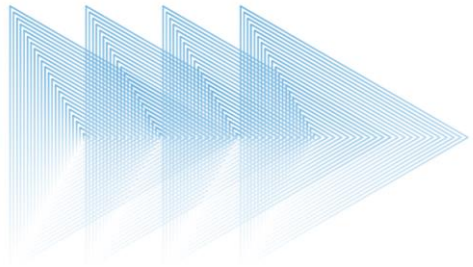
# Theme:

- Meaning of „at cross-purpose”
- Different subjects, diferent purposes

# 1. Theme (1): meaning of „at cross-purpose”

- The overarching theme: Should companies carry out a full-scope ZZPL/GDPR compliance audit and comprehensive implementing measures?
- Short answer: Yes.
- Longer answer:

Continue



# 1. Theme (2): meaning of „at cross-purpose”

Collins: If people are at cross-purposes, they do not understand each other because they are working towards or talking about different things without realizing it.

# 1. Theme (2): diferent subjects; different purposes

## Different subjects

- Law firm
  - considers that proper compliance audit is unusually complex from the legal point of view
  - believes that proper compliance audit can only be done in an integral way
- Some companies
  - do not find it evident that legal complexity of the compliance audit is exceptional;
  - believe that a partial compliance might be good enough, because certain segments of company's activities are inherently more risk-ridden or otherwise more significant than other

# 1. Theme (2): diferent subjects; different purposes

## Different purposes

- Law firm believes a high fee is appropriate, because a proper compliance audit requires significant amount of intellectually demanding work
- Company prefers to have as much compliance as possible, but without spending considerable amounts

BDK Advokati

# Who talks at cross purpose

BDK Advokati

# 2. Who talks at cross-purposes

- Law firms: The presentation is based on our law firm's experience and takes into account feedback from colleagues from other law firms with substantial expertise in data protection law.

- Companies

  – Those committed to full compliance, but unsure of what it requires to achieve one

  – Those that consider partial compliance good enough

  Not falling to either of the above: the companies relying on their own capacities to achieve compliance (e.g. banks and insurance companies)

BDK Advokati

# Attorney's view

# 3. Attorney's view (1) – must have (A)

Proper compliance audit **must** include thorough identification and analysis (expressed in a comprehensive report) of:

- all data processing operations, and
- with regard to each type of processing operation:
  - categories of data processed
  - purpose and proportionality
  - legal basis
  - notice to individuals ('data subjects')
  - legal status of the client ((co-)controller, processor)
  - retention period – actual and permissible
  - access to the data and measures ensuring security of the data
  - agreements with data processors and joint controllers
  - legal basis for cross-border transfer, and transfer agreements
  - internal procedure (for responding to individuals' requests and reporting data breaches)

BDK Advokati

# 3. Attorney's view (2) – must have (B)

Remedial measures **must** include creation of:

- data protection notices
  - employees and contractors
  - other individuals ('data subjects'): job applicants, suppliers and clients (responsible persons at), customers;
  - website visitors (includes creation of cookie notice)
  - visitors of company premises (CCTV)
- agreements with data processors (e.g. providers of IT services)
- agreements with joint controllers
- records of processing activities
- data transfer agreements, where applicable

ZZPL and GDPR explicitly require the above.

BDK Advokati

# 3. Attorney's view (3) – important to have (A)

Remedial measures **should** include creation of:

- procedure for managing and reporting data breaches
  - breach response plan
  - template breach notification letters
  - log for reporting security incidents
- procedure for responding to requests of the individuals
  - templates
  - tracking form
- legitimate interests analysis (document), for the processing based on legitimate interests

Not expressly required by law. However, non-availability of the procedures and documents significantly increases the risk of non-compliance.

# 3. Attorney's view (4) – important to have (B)

Closely related implementing measures **should** include:

- creation of general data protection compliance policy (document)
- creation of a document specifying data retention periods for each processing operation
- training for the relevant company staff on obligations under GDPR/ZZPL

Creation and use of the documents, and the training:

- help demonstrate compliance
- raise awareness.

BDK Advokati

# Client's view

# 4. Client's view

[Reminder: The following does not apply to companies with commitment and capacity to conduct comprehensive compliance audit on their own.]

'*Partial compliance, or even non-compliance, is good enough, because*

- *consequences of non-compliance do not seem to be grave:*
  - *low fines under ZZPL*
  - *DPA might not have capacity or commitment to vigorously enforce ZZPL*
- *in any event, funds are limited*'

'*The fee should be fairly limited, because*

- *no reason to consider that the work requires expertise* that *exceptional, or exceptional investment of time*'

BDK Advokati

# Appraisal of the views

# 5. Appraisal of the views (1)

"'*Partial compliance, or even non-compliance, is good enough, because consequences of non-compliance do not seem to be grave:*

- *low fines under ZZPL*
- *DPA might not have capacity or commitment to vigorously enforce ZZPL*

*in any event, available funds are limited*'"

- It is not about fines first and foremost.

- Business and cultural environments are changing:

  - ➢ compliance as a goal in-and-of itself, an aspect of brand
  - ➢ therefore, companies striving for excellence seek to be recognized as leaders in compliance.

# 5. Appraisal of the views (2)

- Reputational gains –and risks – are significant:
    - customers
    - public at large – rapidly gets more sensitized
    - competitors
    - the group
    - regulatory authorities (excellence in DP compliance ‘buys credit” in other regulatory fields)
- Reputational loss – e.g. massive loss of financial or health data – may turn into loss of customers

# 5. Appraisal of the views (3)

- ZZPL is here to stay, and the present absence of DPA's commitment to implementing the law vigorously is not likely to continue
- DPA can impose low fines; courts do not confront similar restrictions with respect to damages
- Downsides of selective compliance:
  - leaves sectors within the company unsatisfied
  - the remaining work will have to be done, and the total price will be higher

# 5. Appraisal of the views (4)

'*The fee should be fairly limited, because no reason to consider that the work requires expertise that exceptional, or exceptional investment of time*'

- By all means scrutinize lawyers and their claims

  but

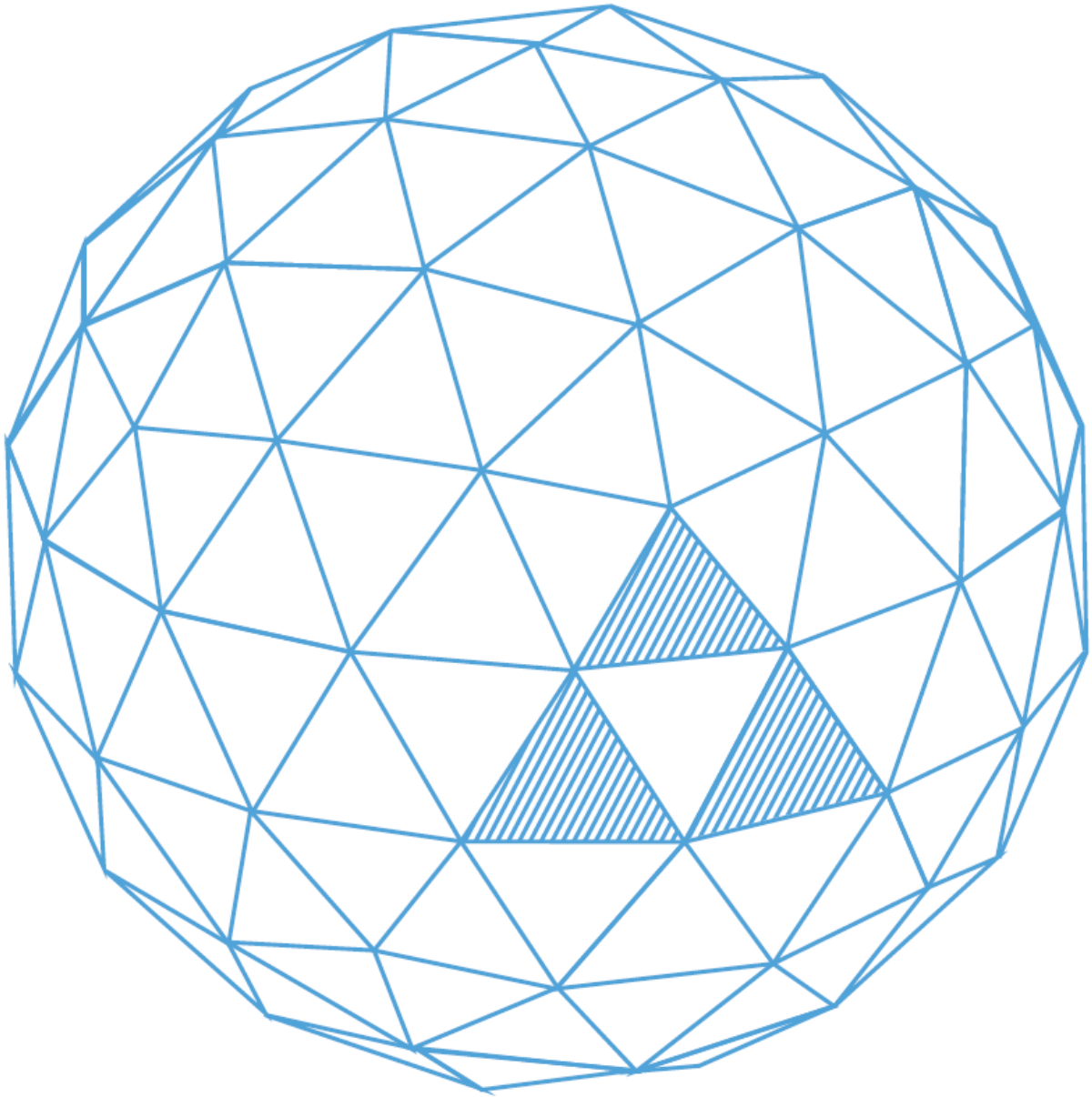
- DP law **is** complex and often lacks obvious 'correct answer'. Leading DPAs often 'answer' the same questions differently (before they sit down to clear up their differences).

# 5. Appraisal of the views (5)

| Issue | France | U.K. | Germany |
|---|---|---|---|
| Territorial scope | In order for consent to be informed, the user must be able to identify all parties processing their data. This means that organizations should name all parties who will rely on users' consent. | | |
| **Differences** | | | |
| Grace period | Yes. Companies are expected to comply with the new rules six months after the publication of a (yet to be issued) opinion from the CNIL discussing how to obtain consent in practice. The CNIL expects this opinion to be in a final form in the course of the first quarter of 2020. | No. | No. |
| Are cookie walls allowed? | No. Cookie walls are not compliant as the user would suffer adverse consequences if they refused to accept. | ICO notes that consent that is forced via a cookie wall is "unlikely to be valid." However, it also notes that GDPR must be balanced against other rights, including freedom of expression and freedom to conduct a business. ICO seems to be "sitting on the fence" on this — at least for the moment. | No, similar to the CNIL. |
| Do analytic cookies require consent? | Not always. Certain analytic cookies can be exempted from prior consent requirements if they meet a list of cumulative requirements provided by the CNIL. | Yes. There is no exception. Though ICO states that it is "unlikely that priority for any formal action would be given to uses of cookies where there is a low level of intrusiveness and low risk of harm to individuals," and first-party analytics cookies are given as an example of cookies that are potentially low risk. | No, unless they lead to a transfer of personal data to a third party. Even in that case, likely no consent would be necessary if users can easily opt out from the data transfer to the third party. |

BDK Advokati

# Conclussion



# 6. Conclusion

- One does not need to be a DP enthusiast or absolutist to recognize that compliance with the DP law will only grow in importance, globally and locally.
- The sooner a company adapts to the trend, the more likely she is to enjoy competitive advantage in the market and occupy favorable position in the hearts and minds of (potential) customers.

**BDK Serbia**
Bulevar kralja Aleksandra 28
11000 Belgrade
Tel: +381 11 3284 212
office@bdkadvokati.com

**BDK Montenegro**
Cetinjska 11, The Capital Plaza
81000 Podgorica
Tel/Fax: +382 20 230 396
office.cg@bdkadvokati.com

**BDK Bosnia and Herzegovina**
Gundulićeva 6
78000 Banja Luka
Tel: +387 51 250 641 Fax: +387 51 250 642
office.banjaluka@bdkadvokati.com

**www.bdkadvokati.com**

SEE A member of Legal