Data Protection Authorities and new information technology

Dr. Ivan Szekely
Eotvos Karoly Policy Institute; Blinken OSA Archivum
szekelyi@ceu.edu

PRICON Conference
The Institute of Economics, Zagreb, 14 May 2018

Functions and roles of DPAs

Flaherty (1997):
- Oversight
- Auditing
- Monitoring
- Evaluation
- Expert knowledge
- Mediation
- Dispute resolution
- Balancing of competing interests

Bennett and Raab (2006):
- Ombudsman
- Auditor
- Consultant
- Educator
- Policy adviser
- Negotiator
- Enforcer

Bieker (2017):
- Enforcement
- Complaints-handling
- Co-operation across DPAs

Schütz (2012):
- Independence

Jóri (2015):
- "Shaping" (privacy advocacy)
- "Applying" (mediating or enforcing)

Hijmans (2016):
- Expert bodies

Functions and roles of DPAs

Estonian DPA survey:

Educational and consultative activities:

- Answering questions
- Adoption of guidance texts
- Approval of self-regulatory acts
- Training sessions and other public events
- Media work, including social media

Policy advising

Additional activities

General competence:

- Data protection and freedom of information

Supervision and enforcement:

- Mediation
- Comparative survey
- Notice without investigation
- Preventive audit
- Registration
- Authorizations re. data transfer to 3rd countries
- Prior checking
- Investigation and resolving of infringements
- Resolutions

Tasks of DPAs in the GDPR*

- Monitor and enforce
- Promote public awareness
- Advise the parliament, the government
- Promote the awareness of controllers
- Provide information to data subjects
- Handle complaints
- Cooperate with other authorities
- Conduct investigations
- Monitor relevant developments
- Adopt standard contractual clauses
- Establish the requirements for DPIA
- Give advice on processing operations
- Encourage: codes of conduct
- Encourage: DP seals and marks
- Review certifications
- Draft the criteria for accreditation
- Conduct the accreditation
- Authorize contractual clauses
- Approve binding corporate rules
- Contribute to the activities of the Board
- Keep internal records of infringements
- Fulfil any other tasks...

*Conducted under 26 specified powers (investigative, corrective, authorization and advisory)

On DPAs and technology

Simitis (1983): these authorities "have the necessary knowledge enabling them to analyze the structure of public and private agencies and to trace step by step their information procedures. They can therefore detect deficiencies and propose adequate remedies."

Flaherty (1989): DPAs "monitor and evaluate new technological developments in data processing and telecommunications. Each agency has specialists in various types of information systems and data flows who can speak intelligently about data protection and security with the operators of government information systems."

Barnard-Wills (2017): Semi-structured interviews with DPAs conducted in the project PHAEDRA II, as well as documentary analysis, showed the variable extent of ICT-related understanding and activity amongst DPAs.

Critical opinions

- DPAs are deficient in their understanding of ICTs;
  their ability to regulate information processing is compromised
  by the deficiencies.

- Both the data controllers and the privacy and human-rights activists
  may have much greater ICT expertise and knowledge than the
  "official" regulators.

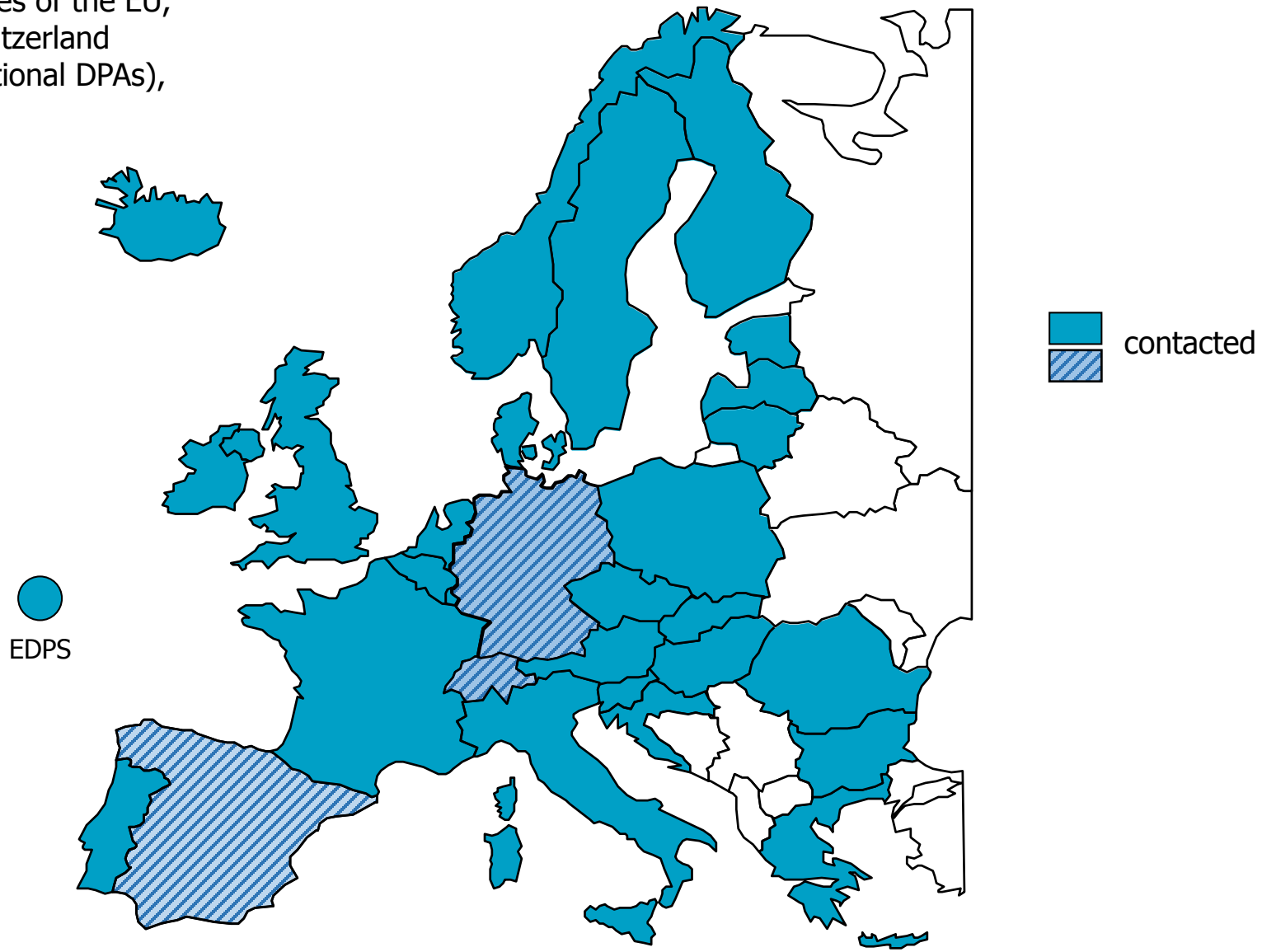
The survey*

- Countries involved:
  Member States of the EU, EEA; Switzerland; EDPS
  (including 32 national and 46 sub-national DPAs)
- Data collection: September-December 2015
- Number of staff of DPAs: 1 to >100
- Response rate:
  47 of 79 DPAs (59.5%)
  including 27 national DPAs (84.4%)
  and 19 sub-national DPAs (41.3%)
  - Replied:
    - competent leaders (22)
    - communications or international depts. (9)
    - IT dept. (2)
    - unknown (11)

* Charles Raab and Ivan Szekely, "Data protection authorities and information technology", *Computer Law and Security Review,* 33 (2017) pp. 421-433.

Countries involved

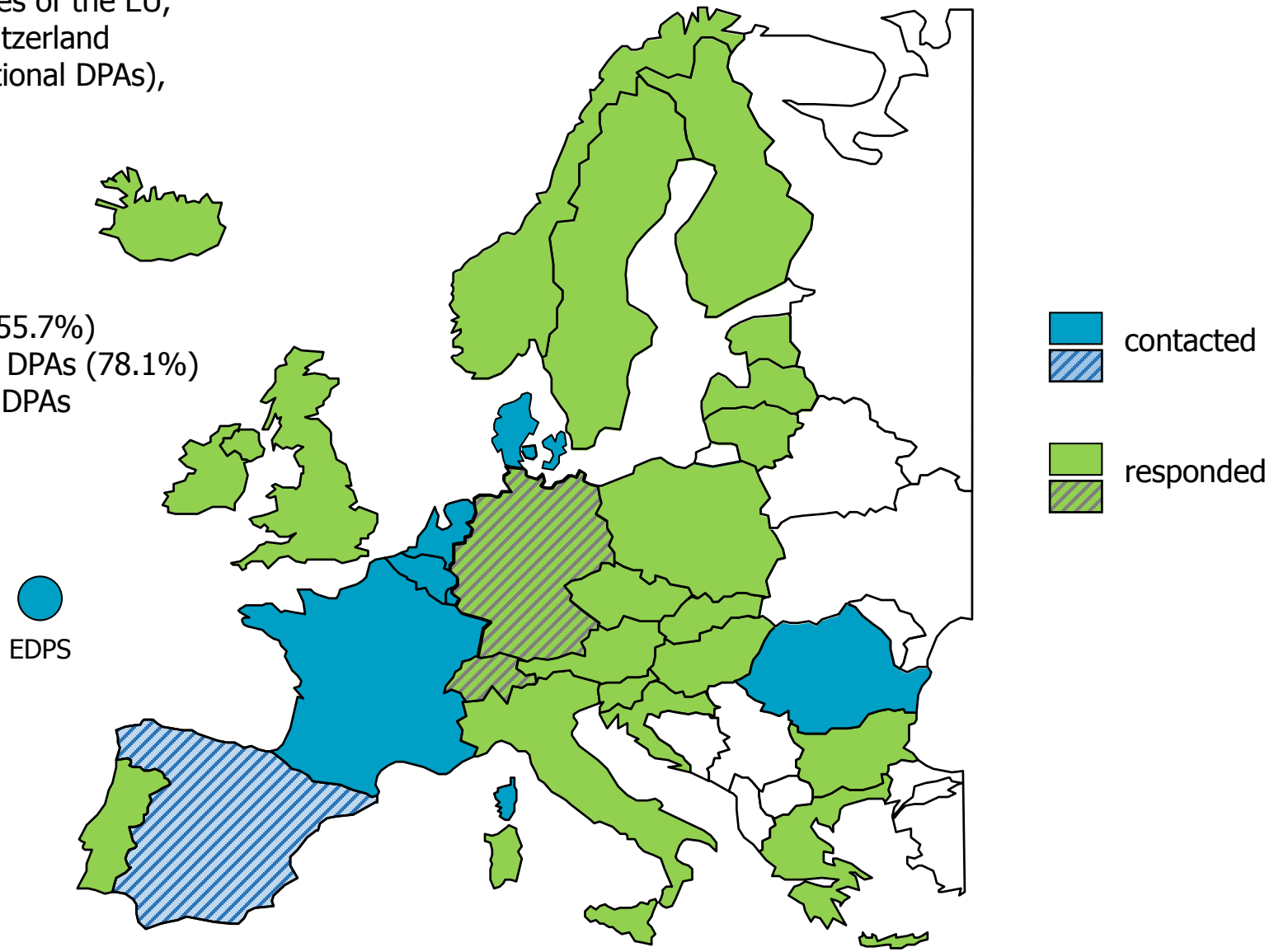
- Member States of the EU, EEA, and Switzerland (incl. sub-national DPAs), + EDPS



Countries responded

- Member States of the EU, EEA, and Switzerland (incl. sub-national DPAs), + EDPS

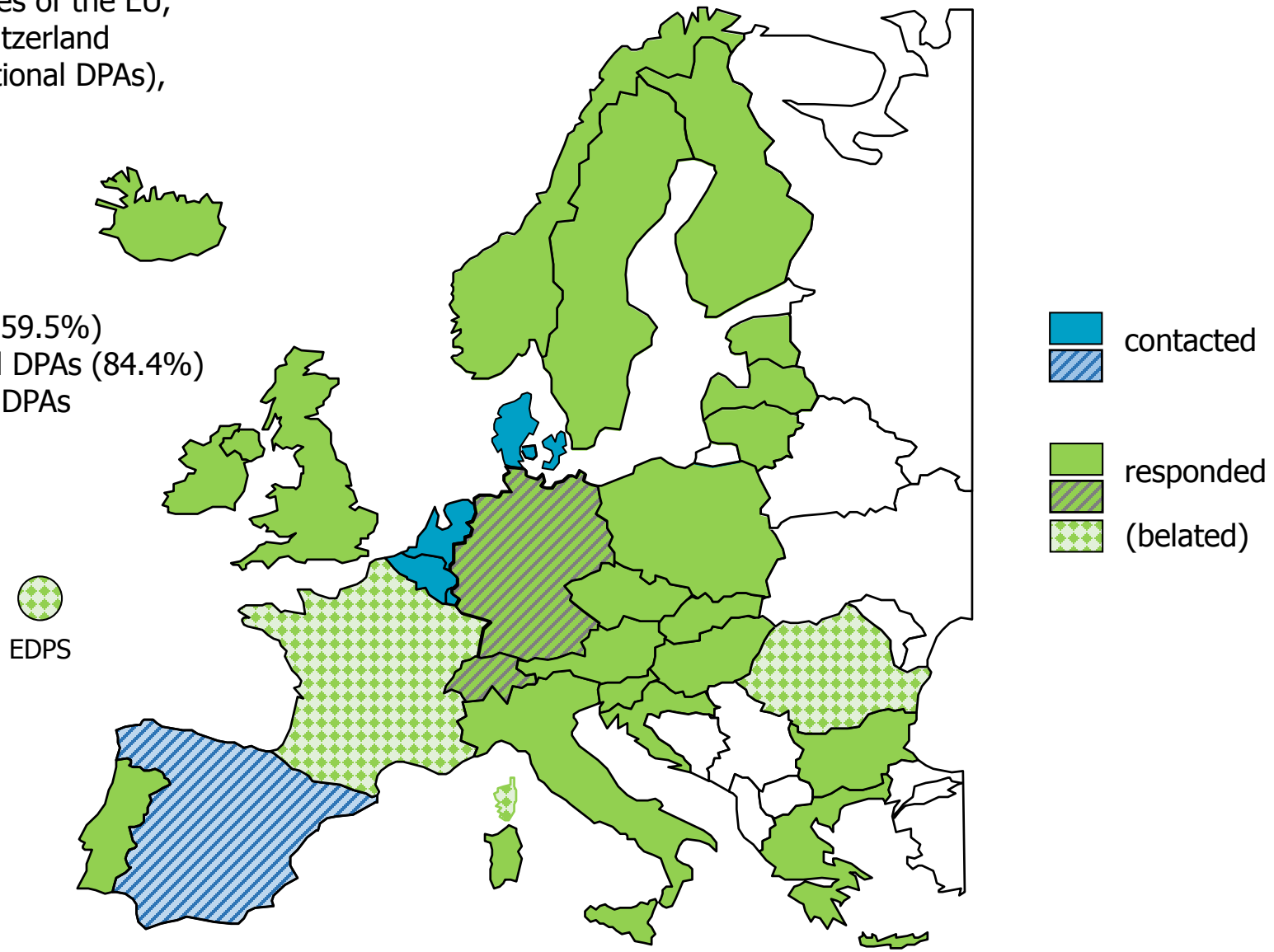
- Response rate:
  44 of 79 DPAs (55.7%)
  incl. 25 national DPAs (78.1%)
  19 sub-national DPAs (41.3%)

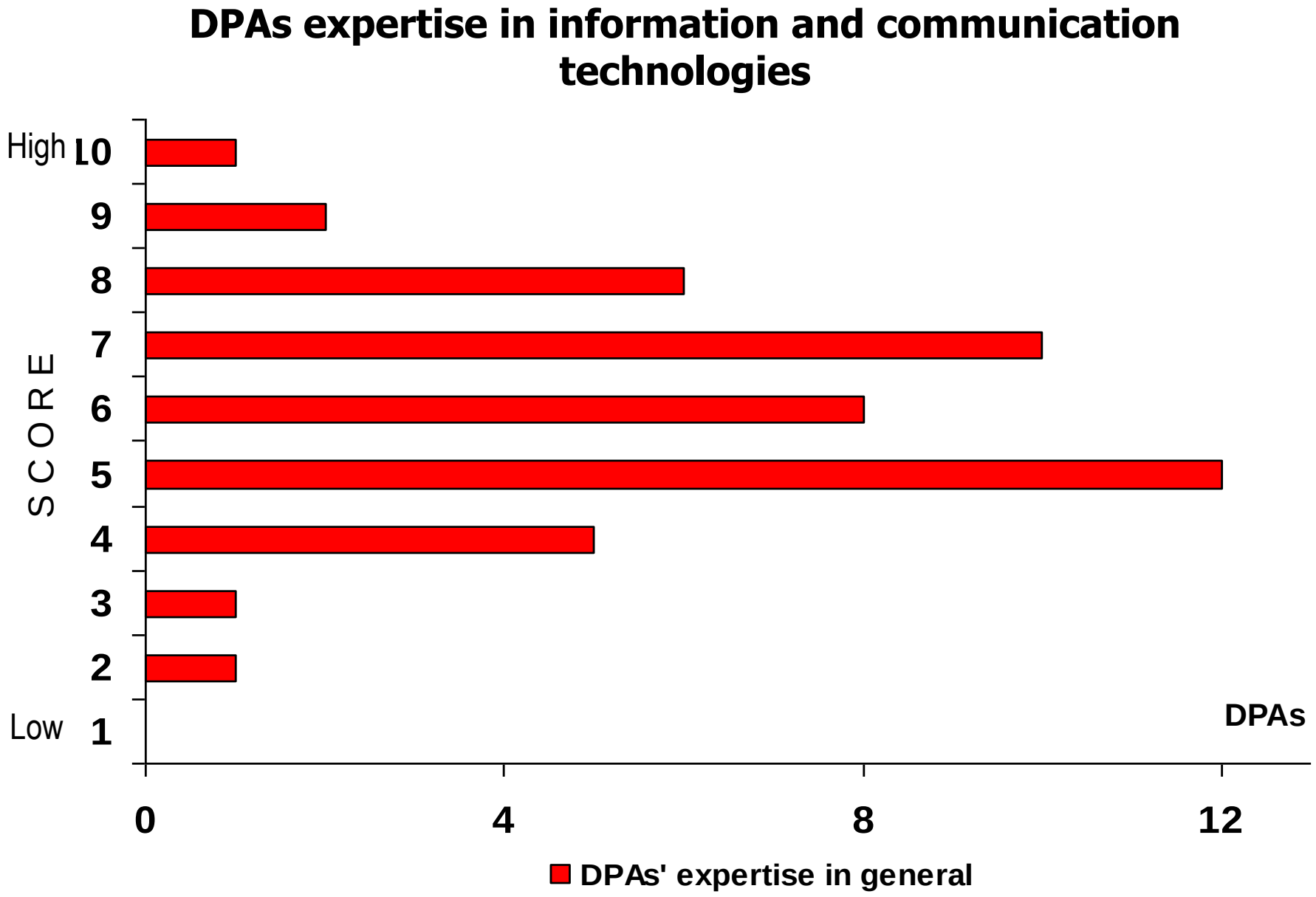


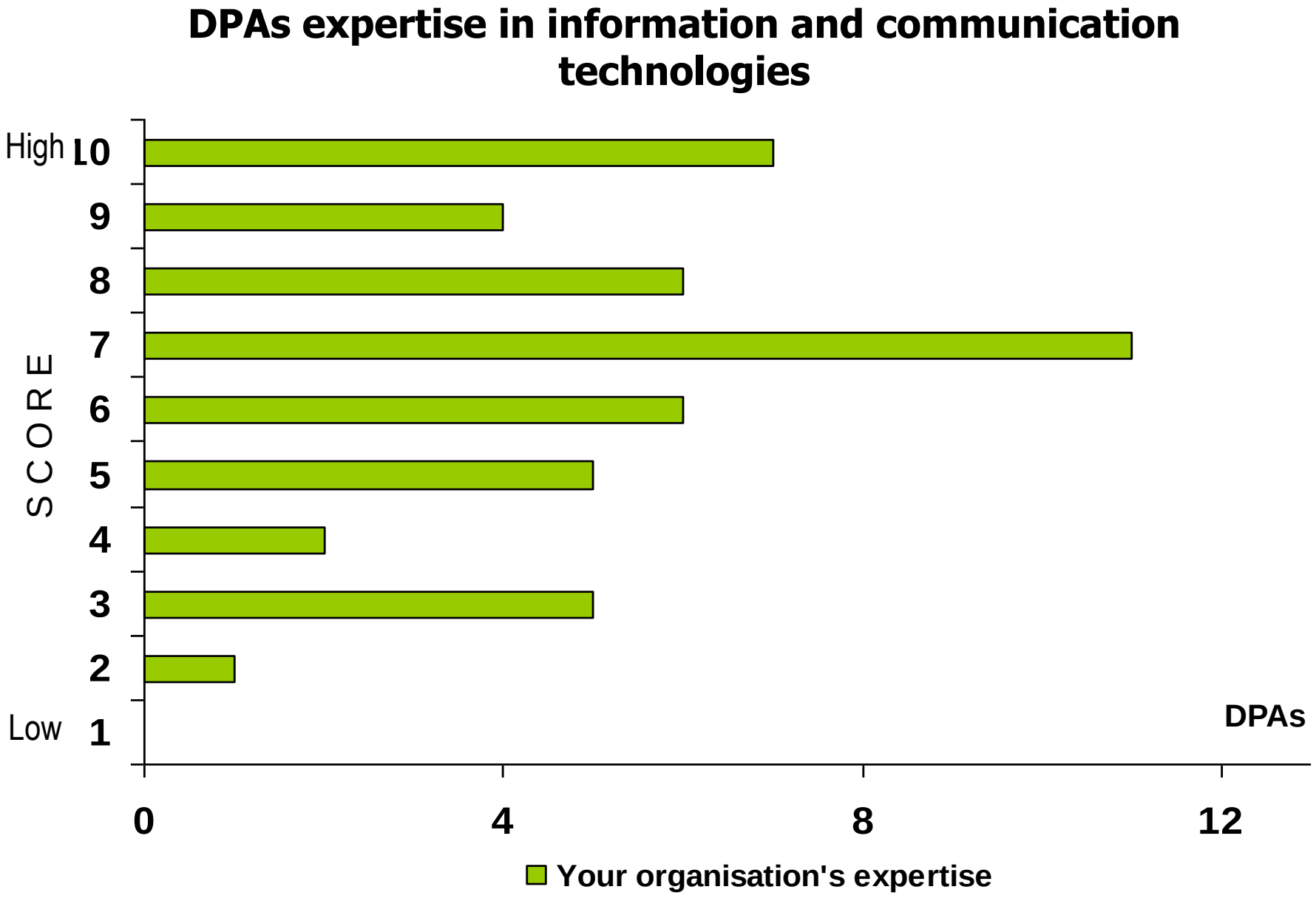
Countries responded (updated)

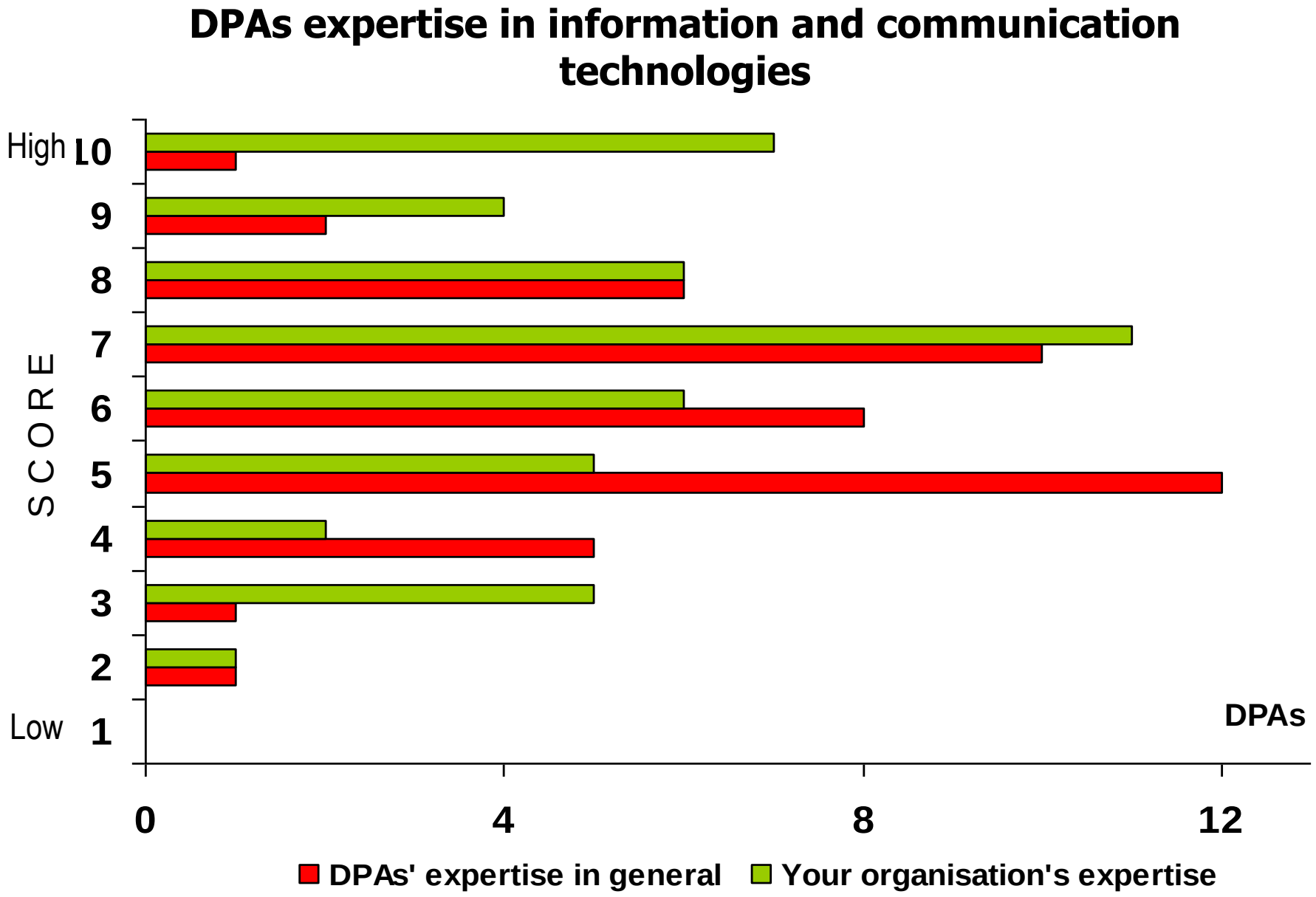
- Member States of the EU, EEA, and Switzerland (incl. sub-national DPAs), + EDPS

- Response rate:
  47 of 79 DPAs (59.5%)
  incl. **27** national DPAs (84.4%)
  19 sub-national DPAs (41.3%)

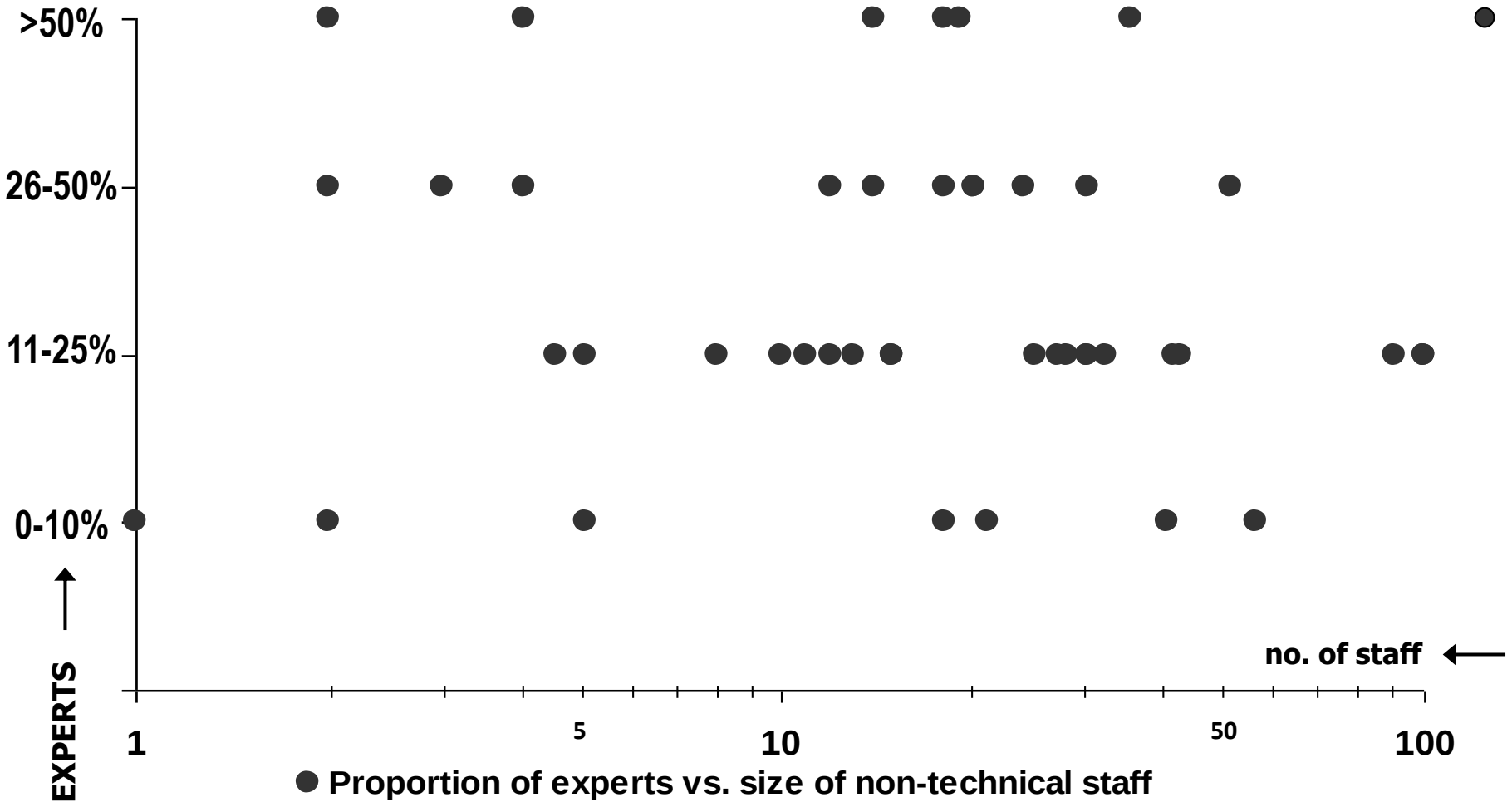



DPAs expertise in information and communication technologies
High
10
9
8
7
6
5
4
3
2
Low
1
SCORE
DPAs
0
4
8
12
DPAs' expertise in general

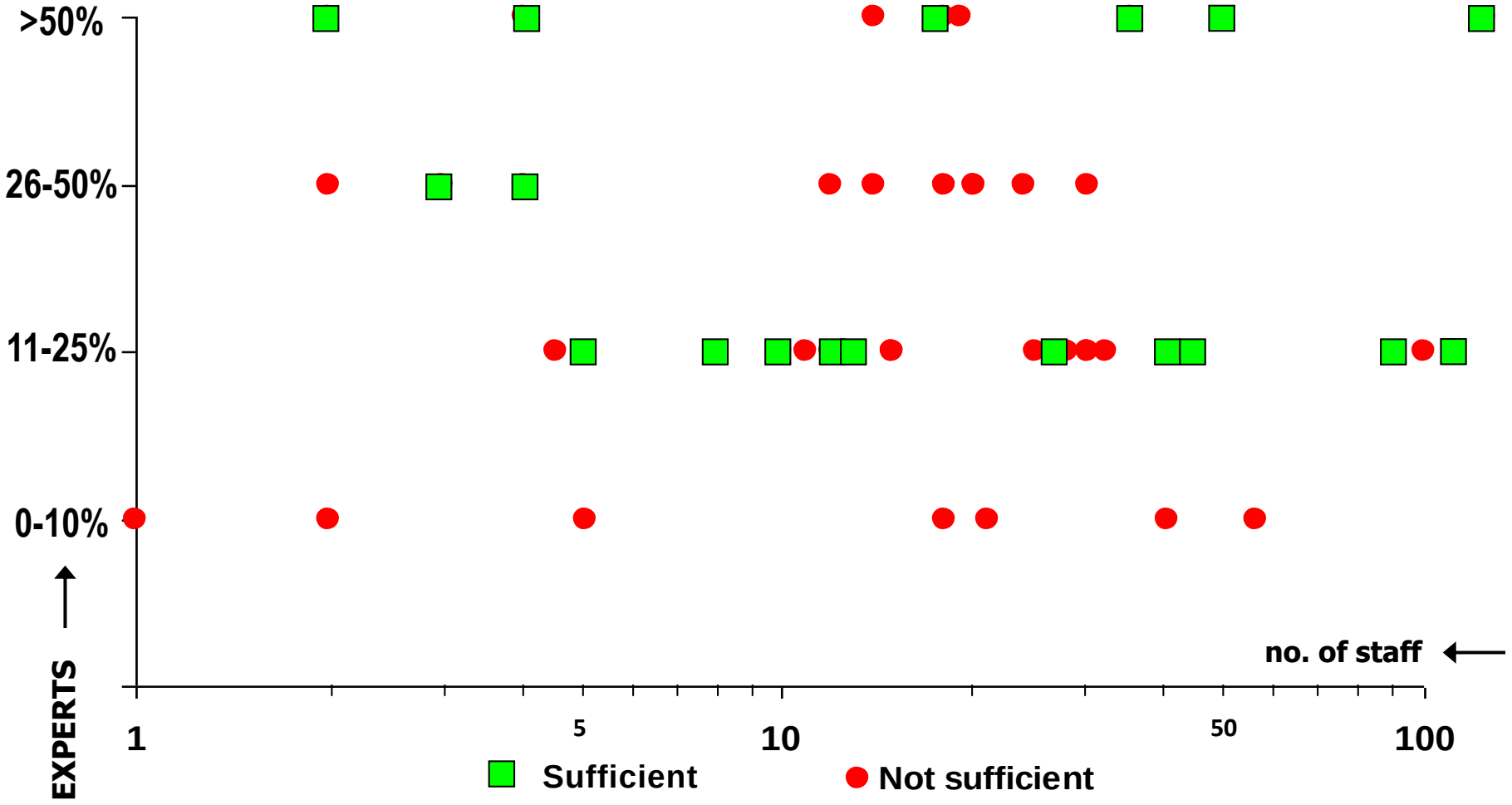

DPAs expertise in information and communication technologies
High
10
9
8
7
6
5
4
3
2
Low
1
SCORE
DPAs
0
4
8
12
Your organisation's expertise


DPAs expertise in information and communication technologies
High
10
9
8
7
6
5
4
3
2
Low
1
SCORE
DPAs
0
4
8
12
DPAs' expertise in general
Your organisation's expertise

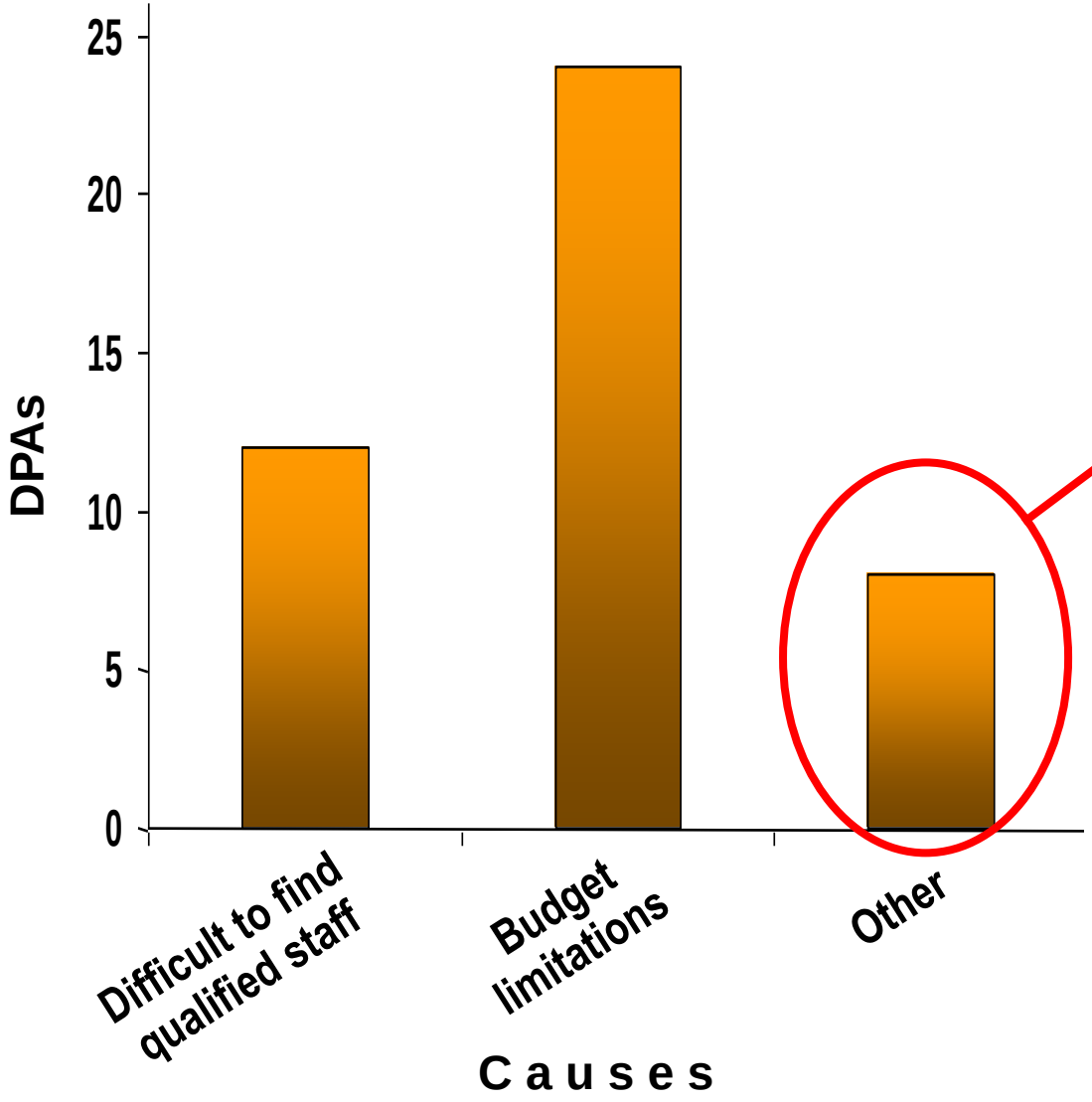
ICT expertise of non-technical staff at DPAs



ICT expertise of non-technical staff at DPAs



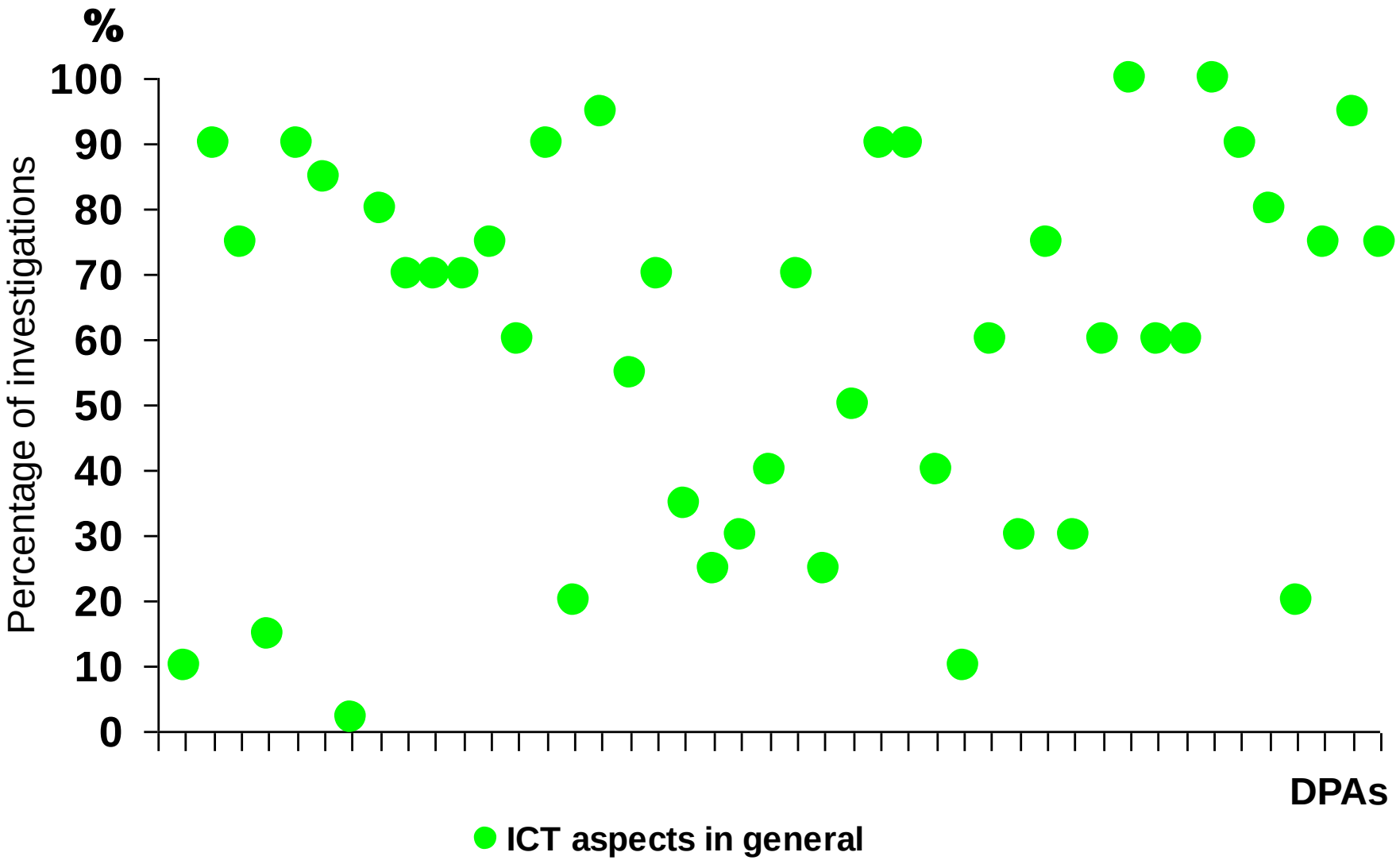
Not sufficient expertise: Causes of the shortfall



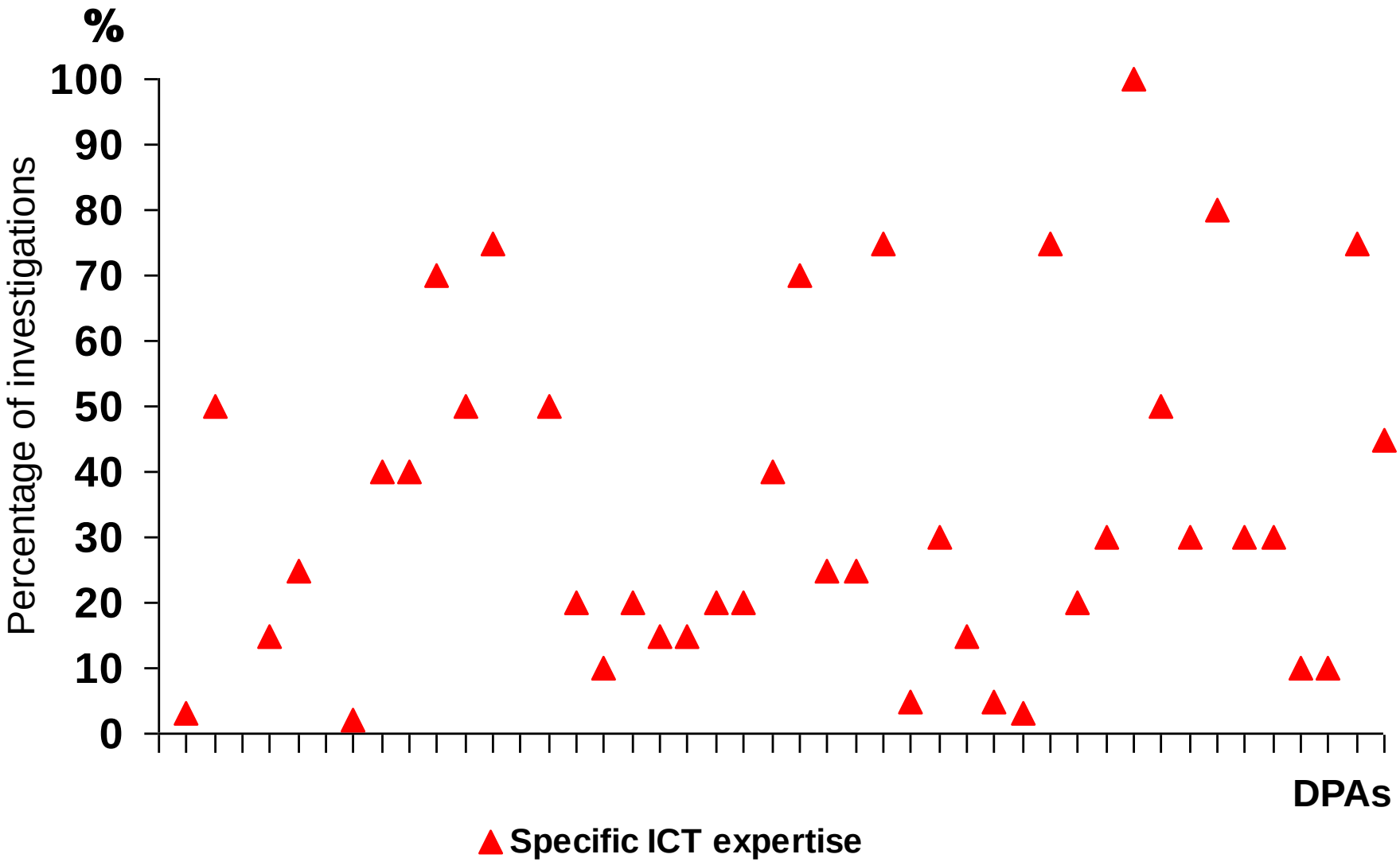
Other:

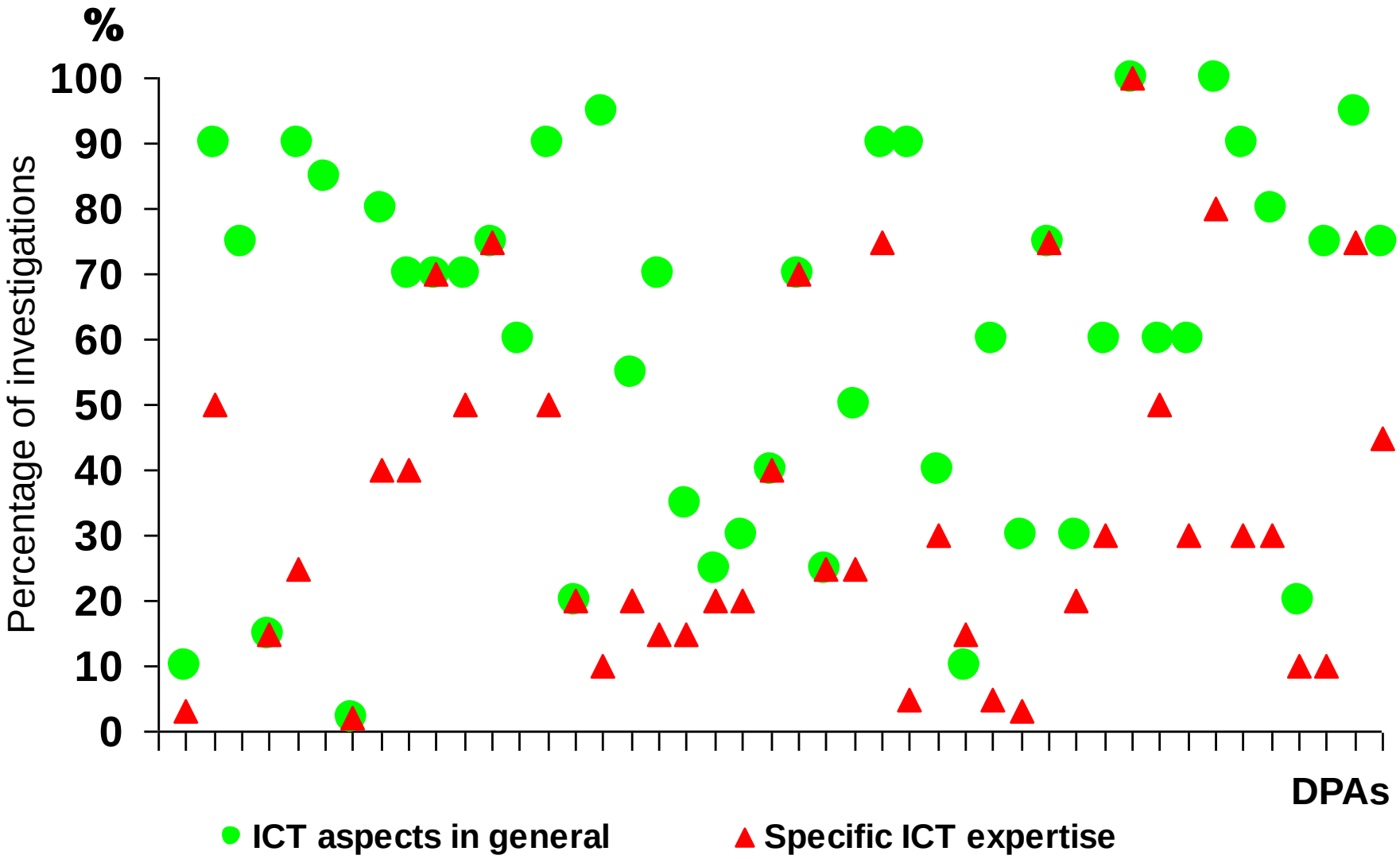
- limited training time available
- preference for hiring legal staff
- low public sector salaries for IT people
- need for trained IT staff greater than available supply

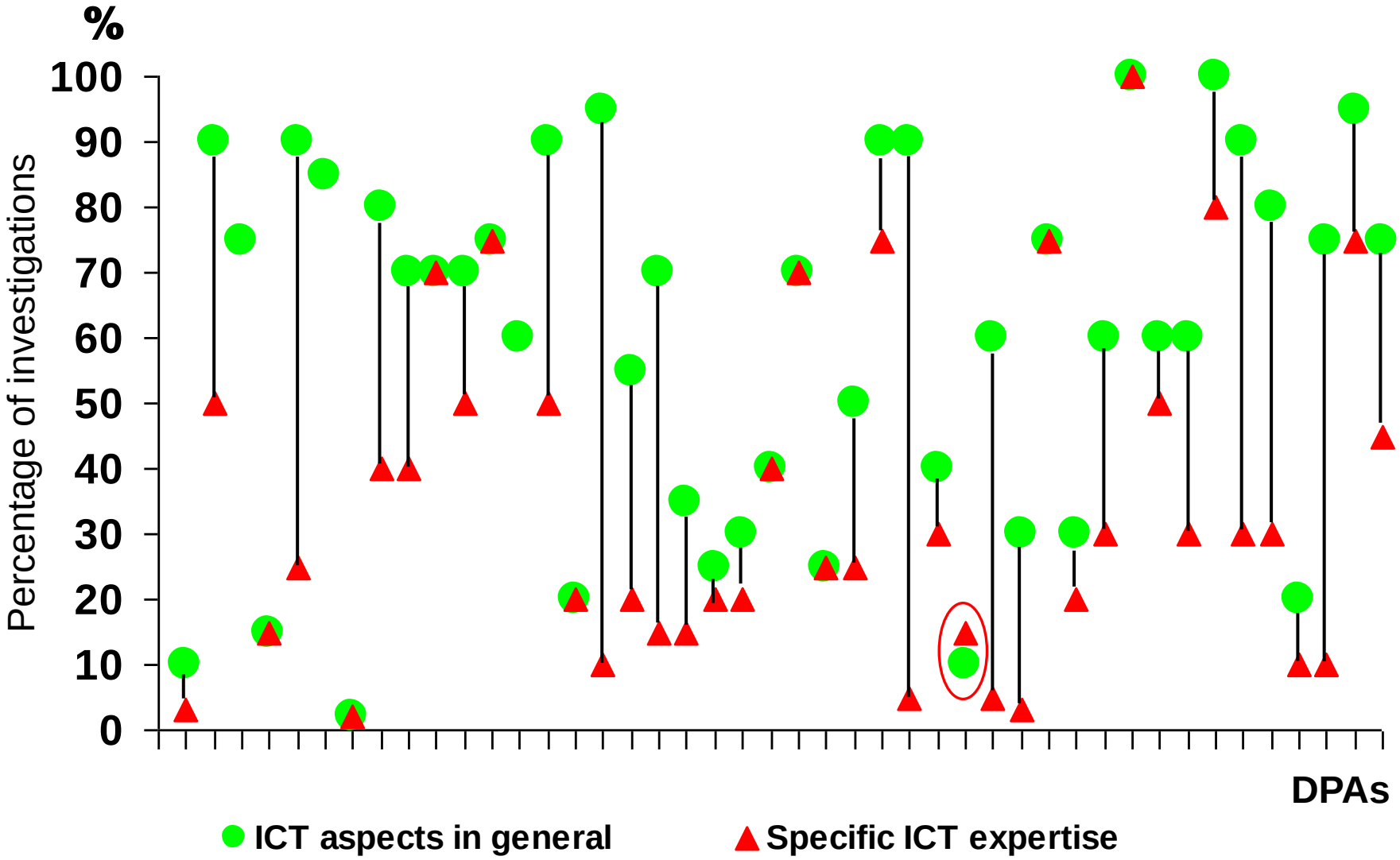
DPA investigations involving ICT aspects *in general*



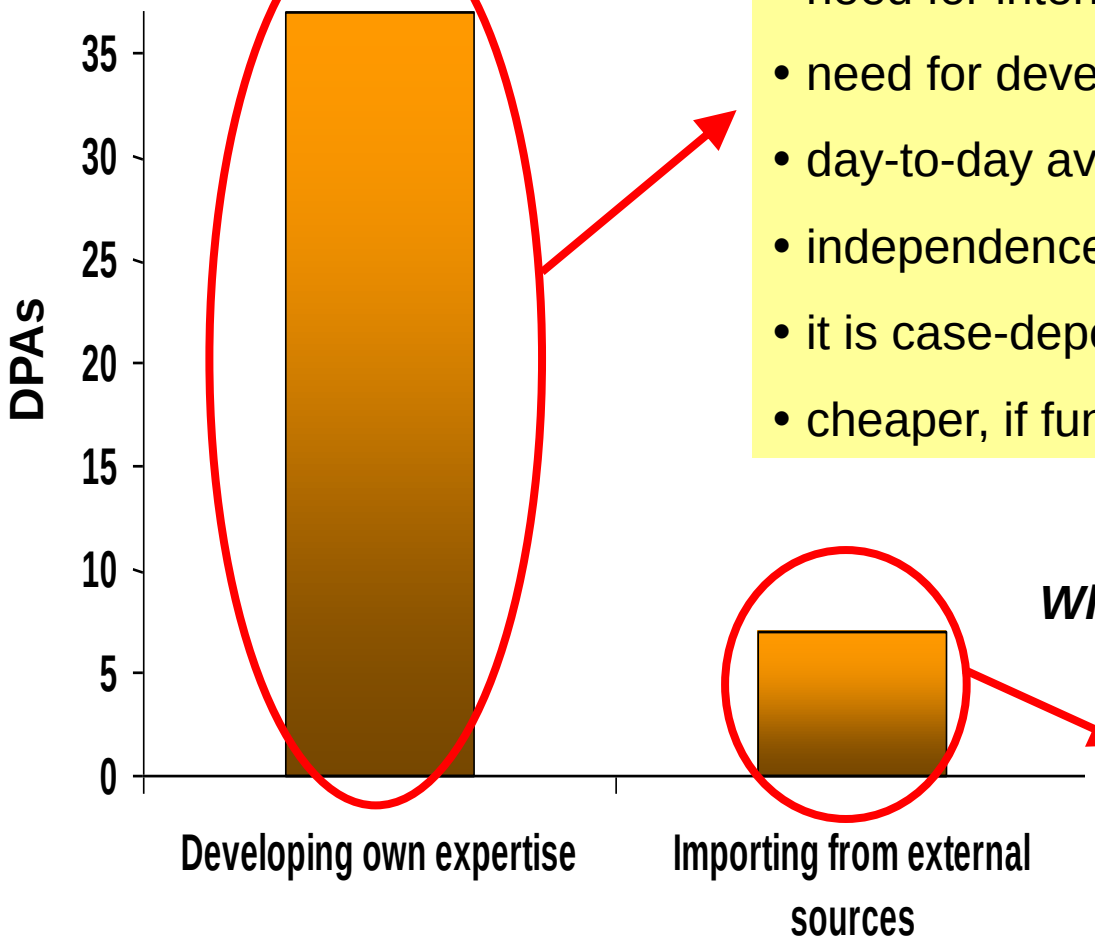
DPA investigations requiring *specific* ICT expertise




DPA investigations involving ICT aspects *in general* and those requiring *specific* ICT expertise
%
100
90
80
70
60
50
40
30
20
10
0
Percentage of investigations
DPAs
ICT aspects in general
Specific ICT expertise


DPA investigations involving ICT aspects *in general* and those requiring *specific* ICT expertise
%
100
90
80
70
60
50
40
30
20
10
0
Percentage of investigations
DPAs
ICT aspects in general
Specific ICT expertise

Developing own ICT expertise or importing from external sources



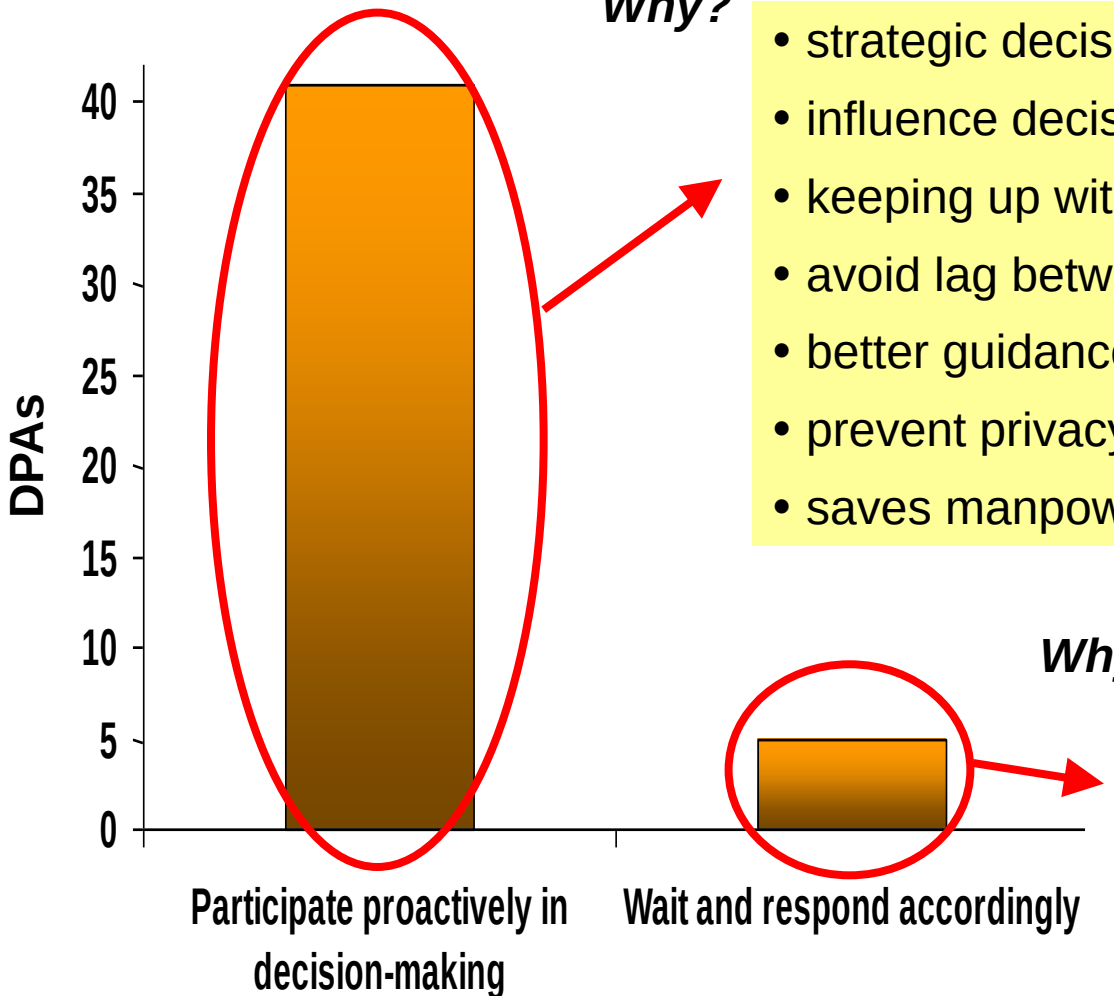
Why?

- need for internal specialised DP knowledge
- need for developing IT knowledge within DPA
- day-to-day availability, proactivity
- independence, impartiality
- it is case-dependent
- cheaper, if funds available

Why?

- up-to-date, higher level of expertise
- special tasks, when needed
- DPA is too small

Proaction or responding



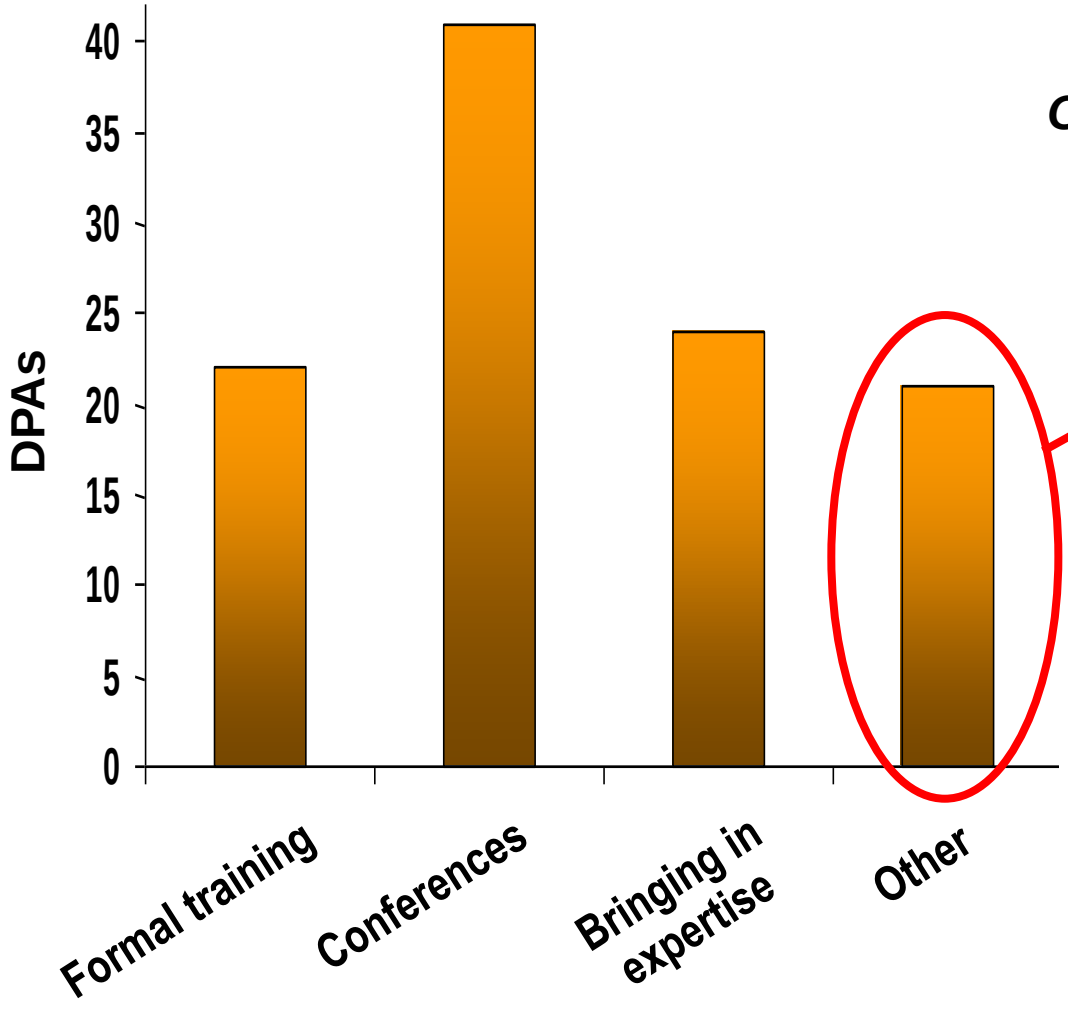
Why?

- strategic decision-making more effective
- influence decisions, PbD
- keeping up with FETs
- avoid lag between issue and response
- better guidance, co-operation with controllers
- prevent privacy breaches
- saves manpower better than if responsive

Why?

- limited resources
- act only when challenge is clear
- not involved in legislation

Keeping up with new developments in ICT



Other:

- reading, studying
- learning on job, in-house informal training
- academic and business community assistance
- interchange with other DPAs
- participation in projects

“Most relevant privacy-related technologies”

◆ mobile devices; smart devices; internet of things ◆ Online identities, identity thefts and data breaches. Monitoring and surveillance technologies. Internet of things; profiling. ◆ Biometrics, smart metering, the internet of Things, Social Networks, search engines and internet services for the publication of videos ◆ Technologies or applications that do not inform users. Under the new Regulation, mechanisms for informed consent and privacy by design/default. ◆ Biometrics, social networks, drones ◆ (1) Information society services and applications: social networks, search, e-commerce, online media;(2) location based and/or tracking services: WiFi, GPS, iBeacons and BLE Beacons, in general telematics;(3) mHealth e.g. telemedicine, wearable (medical) devices; (4) Big Data analytics, smart meters ◆ Totally new ecosystem ◆ Mobile Applications for Smartphones, Tracking Technologies on Websites and Smartphones, Big Data, RFID/NFC ◆ Big Data, Deep learning. DPAs are not very familiar with this coming up technology. ◆ Mobile and cloud-based computing, file-sharing, location-based apps * Genetics, sensor technology, smart cities and smart homes, drones. ◆ cloud computing, big data, mobile computing, smart devices, pervasive computing ..., easy use of cryptography as safeguard for security & privacy ◆ big data applications using self-learning algorithms ◆ 1) Cloud of Things; 2) Industry 4.0, incl. Network Technologies; 3) Smart Systems 4) Big Data; 5) Predictive Computing; 6) ITIL, PRINCE2 etc; 7) Consumer Protection ◆ Internet of Things, Cloud Computing and Big Data ◆ Privacy by Design technologies & applications; big data, cyber physical systems (sensor communication), scoring, authentication & identification technology; all technologies & applications that are part of standard development tools ◆ Ubiquitous computing, internet of things ◆ IoT, Big Data, eID, ICT Security, eGov applications ◆ Big Data analitics, biometrics, location tracking and geolocation based services, behavioral advertisements. ◆ The Internet of things and Big data ◆ BigData processing - "compatible" use; Use and context of smart devices; GDPR; international transfers ◆ Big data, cyber security, mobile app in health sector, profiling, internet of things ◆ The one's that will be used the most. Currently we see that complaints are more related with the broadly used ICT. ◆ IoT, Cloud Computing, PII data flows and PbD ◆ smart grid, broad use of biometrics, video survey and profiling are most significant impact on privacy in general and on DPA's activity - internet for direct marketing, video survey and profiling ◆ biometry, health apps, people tracking and profiling activities, assessments of DPIAs, assessments of Privacy by Design approaches. ◆ The massive data gathering from Internet use and connected devices, and the use of this information beyond the data subjects knowledge and understanding, such as Big Data analyses. ◆ Data exchange technologies, smart grid, Internet of Things, wearable computing ◆ The combination of technologies and the ever higher computing capabilities. ◆ Biometrics, video surveillance, social media, drones, GPS ◆ drones, smart video analytics, internet of things ◆ Cloud services e.g. health care, IoT, Mobil Apps ◆ The data controller's attitude to assessing the data protection and privacy risks in new or existing projects. Privacy Impact Assessment will help identify such risks ◆ There are numerous threats it is not possible to identify one. ◆ Ubiquitous computing / Internet of Things / Big Data / Predicting Profiling / Tracking technologies + Surveillance ◆ Internet and mobile devices (smart phones etc.), technologies of surveillance and detection used by governmental bodies like police, intelligence services etc. ◆ BIG Data ◆ Sensors ◆ Social media, videosurveillance ◆ drones, robotics, autonomous cars, connected things ◆ Big databases with a lot of personal data and a lot of different authorities who are authorized to use it ◆ Cloud Computing; Internet of things; big data ◆ applications such as search engines, analytics tools etc. ◆

“Most relevant privacy-related technologies”

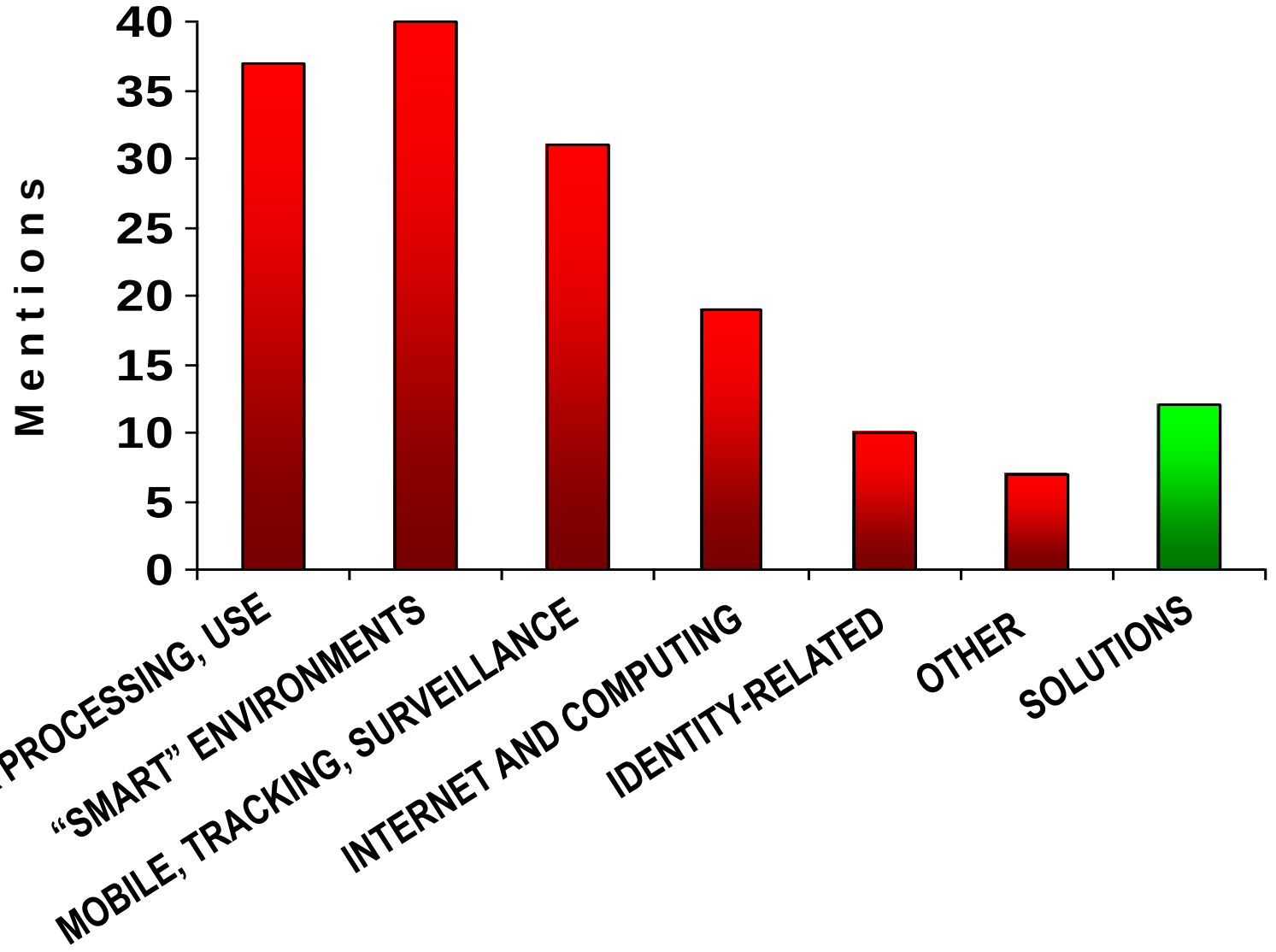
➔ 68 separate technologies/applications/uses mentioned
(62 “risks” + 6 “solutions”)

➔ mentioned altogether 152 times
(in average 2.2 mentions/technology)

➔ by 43 DPAs
(in average 3.5 technologies/DPA)

◆ mobile devices; smart devices; internet of things ◆ Online identities, identity thefts and data breaches. Monitoring and surveillance technologies. Internet of things; profiling. ◆ Biometrics, smart metering, the internet of Things, Social Networks, search engines and internet services for the publication of videos ◆ Technologies or applications that do not inform users. Under the new Regulation, mechanisms for informed consent and privacy by design/default. ◆ Biometrics, social networks, drones ◆ (1) Information society services and applications: social networks, search, e-commerce, online media;(2) location based and/or tracking services: WiFi, GPS, iBeacons and BLE Beacons, in general telematics;(3) mHealth e.g. telemedicine, wearable (medical) devices; (4) Big Data analytics, smart meters ◆ Totally new ecosystem ◆ Mobile Applications for Smartphones, Tracking Technologies on Websites and Smartphones, Big Data, RFID, [illegible] and cloud-based computing, file-sharing, location-based apps.* Genetics, sensor technology, smart cities and smart homes, drones. ◆ cloud computing, big data, mobile computing, [illegible], easy use of cryptography as safeguard for security & privacy ◆ big data applications using self-learning algorithms ◆ 1) Cloud of Things; 2) Industry 4.0, incl. Network Technologies; 3) Smart Systems 4) Big Data; 5) Predictive Computing; 6) ITIL, PRINCE2 etc; 7) Consumer Protection ◆ Internet of Things, Cloud Computing and Big Data ◆ [illegible] cyber physical systems (sensor communication), scoring, authentication & identification technology; all technologies & applications that are part of standard development tools ◆ Ubiquitous computing, internet of things, Big Data, [illegible] Big Data analitics, biometrics, location tracking and geolocation based services, behavioral advertisements. ◆ The Internet of things and Big data ◆ BigData processing - "compatible" use; Use and context of smart devices; GDPR; international transfers ◆ Big data, cyber security, mobile app in health sector, profiling, internet of things ◆ The one's that will be used the most. Currently we see that complaints are more related with the broadly used ICT. ◆ IoT, Cloud Computing, PII data flows and PbD ◆ smart grid, broad use of biometrics, video survey and profiling are most significant [illegible] ◆ Internet for direct marketing, video survey and profiling ◆ biometry, health apps, people tracking and profiling activities, assessments of DPIAs, assessments of Privacy by Design approaches. ◆ The massive data gathering from Internet use and connected devices, and the use of this information beyond the data subjects knowledge and understanding, such as Big Data analyses. ◆ Data exchange technologies, smart grid, Internet of Things, wearable computing ◆ The combination of technologies and the ever higher computing capabilities. ◆ Biometrics, video surveillance, social media, drones, GPS ◆ drones, smart video analytics, internet of things ◆ Cloud services e.g. health care, IoT, Mobil Apps ◆ The data controller's attitude to assessing the data protection and privacy risks in new or existing projects. Privacy Impact Assessment will help identify such risks ◆ There are numerous threats it is not possible to identify one. ◆ Ubiquitous computing / Internet of Things / Big Data / Predicting Profiling / Tracking technologies + Surveillance ◆ Internet and mobile devices (smart phones etc.), technologies of surveillance and detection used by governmental bodies like police, intelligence services etc. ◆ BIG Data ◆ Sensors ◆ Social media, videosurveillance ◆ drones, robotics, autonomous cars, connected things ◆ Big databases with a lot of personal data and a lot of different authorities who are authorized to use it ◆ Cloud Computing; Internet of things; big data ◆ applications such as search engines, analytics tools etc. ◆

"Most relevant privacy-related technologies"



Conclusions

- Great differences among DPAs in:
  - the importance of ICT
  - the nature of their investigations
  - their ICT expertise
  - their approaches to influence technological developments
  - their available resources

- Most relevant privacy-related technologies = “everything”

Conclusions – public discussion

- The technical expertise of European DPAs in general is *not adequate* for the challenges of today and the foreseeable future
- It is best if DPAs develop the necessary technical expertise in-house
- No benchmark in ICT expertise:
  - difficult to evaluate
  - comparison between DPAs debatable
- For the majority of the data controllers it is better if DPAs participated proactively in ICT-related strategic decision-making
- Data controllers, esp. service providers *can* mislead DPAs in ICT-related matters (but they do this only infrequently, because they are afraid of the risks)

Suggestions

Set up a center where ICT experts from DPAs' offices are registered and DPAs could exchange them for a limited time period. It could be an extension of the European Data Protection Board which is to be set up under the GDPR.

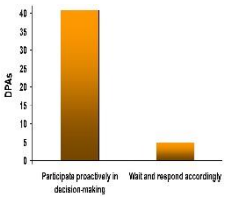
Involve representatives from industry in discussions of new data processing technologies and their impact on privacy and data protection. (However, moderation should remain in the hands of DPAs.)

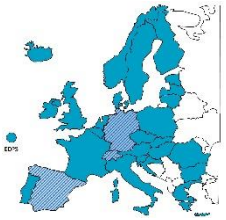
- The London Initiative:
  (28th International Conference of Data Protection and Privacy Commissioners, 2006)
  "Commissioners should reinforce their capacities in technological areas... The excessively 'legal' image of data protection must be corrected."

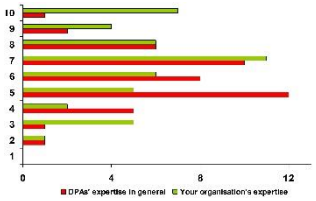
Thank you for your attention!

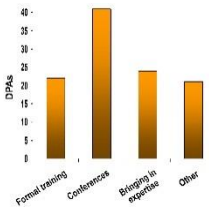
Dr. Ivan Szekely
szekelyi@ceu.edu

DPAs and New Information Technology









Q&A