LIST OF POWERS, ACTIVITIES and STATISTICS of DATA PROTECTION AUTHORITIES

Reporting year: 2016

1. GENERAL INFORMATION and COMPETENCE

1.1. General information

Name of the country:
Estonia

Name of the authority:
Andmekaitse Inspektsioon (Data Protection Inspectorate)

Territorial competence in the whole country
1. Yes
2. No

If the previous answer was No, then in which territory:

Explanation: the description of territory includes also – if relevant – short comments on territorial differences in substantive competence (e.g.: data protection and spam competence in the whole country, FoI competence only in some parts of the country).

Annual budget of the reporting year in euros:
700. 821 €
(Supporting services like IT, bookkeeping, human resources are provided by supporting agencies and are not included into our budget)

Staff (annual average) in full-time-equivalents of the reporting year:
18
(Supporting staff of supporting agencies is not included. Housekeeping is provided by private contractors)

The authority is led by
1 single Head
2 College of Commissioners

1.2. Data protection competence

Legal competence in the scope of the Directive 95/46/EC and Framework Decision 2008/977/JHA (respectively for EDPS – the Regulation 45/2001):

Coverage of the entire scope of both the legal instruments
1 Yes
2 No
If No – description of the limited scope

Comments:

Explanation: Please give the description of a limited scope using general terms as much as possible,

without specific national terminology (e.g.: private sector only, federal public sector only).

Territorial limitations are described in the sub-chapter 1.1.

The matters should not be taken into account in the description of a limited scope if they are also outside of the scope of the Directive according to the Art. 3 (2): like public security, defence, State security and activities of the State in areas of criminal law.

Possible exceptions mentioned in Art. 9 of the Directive (freedom of expression) should also not be taken into account in the description of a limited scope.

Next 2 questions are reserved for the exclusions under Art. 3 (2) and exceptions under Art. 9 of the Directive.

Activities outside of the data protection, spam matters and freedom of information are described under 5. Chapter "Additional activities".

Brief description of the DPA's data protection competence in the areas, excluded from the scope of the Directive according to the Art. 3 (2): first of all public security, defence, State security and activities of the State in areas of criminal law.

Estonian DPA has competence in areas of criminal law and court procedure with the specifications and derogations provided by procedural law.
Estonian DPA has competence in areas of public and national security and defence – except the processing of State secrets (classified information for national security purposes). However, this exception cannot applied in supervisory activities concerning Schengen and Europol information.

Explanation: Please describe here briefly the substantial competence, not procedures. Chapter 3 ("Supervision and enforcement activities") covers also possible procedural exceptions related to the areas mentioned in the Art. 3 (2) of the Directive.

Brief description of the DPA's data protection competence in the matters of journalism and freedom of expression:

Estonian DPA has competence in the matters of journalism and freedom of expression. It involves criteria of predominant public interests, ethics of journalism and excessive damage.

Explanation: Please describe here briefly the substantial competence, not procedures. Chapter 3 ("Supervision and enforcement activities") covers also possible procedural exceptions related to journalism and freedom of expression area according to the Art. 9 of the Directive.

1.3. Competence in spam matters and in telecom data breach cases

Legal competence in the area of unsolicited communications (spam matters) - according to Article 13 of the Directive 2002/58/EC (as amended in the directive 2009/136/EC):

1 In the whole scope
2 Not at all (data protection matters only)
3 If partially, then in which matters:

Comments:

Automated messages only – human-to-human phone calls not included

Additional competence in case of telecom data breaches - to act as the competent national authority according to the Art. 4 of the Directive 2002/58/EC (as amended in the directive 2009/136/EC):

1 Yes
2 No
3 If partially, then how:

Comments:

Explanation: if the DPA is exercising its usual supervisory competence in relation to use of personal data in the unsolicited communications, then it will not be taken into account under spam matters.

Spam matters are distinctive from data protection matters because the Article 13 of the Directive 2002/58/EC contains specific rules for unsolicited communications like opt-in and opt-out rules, easy unsubscribe option rule.

These rules will be applied despite of the fact of who the addressee of unsolicited communications is (an identified or identifiable natural person, a legal person or an unidentified or unidentifiable person). Data protection rules cover only data of identified or identifiable natural persons.

1.4. Competence in the freedom of information matters

Legal competence in the area of supervision over responding to information requests – according to Art. 8 of the pending Convention of the Council of Europe on Access to Official Documents of 2009

1 Yes
2 No

Comments:

If you answered Yes to the previous question, then does the DPA also have competence to supervise information holders in the matters of:
a) disclosure of public sector information on the web

1 Yes
2 No

Comments:

b) protection of restricted information – if restricted information has been revealed then does the DPA have the competence at least to investigate it (even if the revealed information does not contain personal data)?

1 Yes
2 No

Comments:

c) machine-readability of public sector information in the meaning of the Art. 5 of Directive 2013/37/EU on re-use of public sector information

1 Yes
2 No

Comments:

Explanation: If the DPA is merely exercising its usual personal data protection competence within public sector information, then it is not taken into account under freedom of information (FoI) competence.

All questions on access to and re-use of public sector information above cover also sector-specific legislation like in the field of access to environmental information (see the Århus Convention of 1998 and Directive 2003/4/EC).

1.5. Principal legal and organisational developments

Principal legal and organisational developments in the reporting period

Supervisory competence over public sector registers – tasked by the Parliament in January of 2016.
Official internal structure was abolished and structural unites (departments) were dissolved in September of 2016. Now all employees are direct subordinates to the Head of the DPA.
There are unofficial working groups instead of departments.

1.6. Highlights in case law

Highlights in case law in the reporting period

2. EDUCATIONAL and CONSULTATIVE ACTIVITIES

2.1. Activity: answering questions

Statistics of the reporting year: recorded answers:

2836

If applicable: how the total above is divided between data protection, spam and FoI matters

2284 data protection (small number of spam matters included) + 436 FoI matters

Explanation: all recorded answers should be taken into account (including by e-channels and by phone).

Answers to the journalists should also be taken into account (even if they get dealt with separately).

Complaints are not taken into account as questions. E.g. if a data subject asks what he has to do in order to execute his access right to his personal data and the answer he is given is classed as 'advice', then what he should do next is a usual question. If the DPA takes the address as an announcement about violation of the law and subsequently opens an investigation, then it can be qualified as a complaint.

Any person can ask questions. It is not reasonable for common basic statistics to identify the exact role of the person: data subject, data controller/processor, FoI requester, journalist, academic researcher or just a curious person. Therefore all answers have to be included into statistics, not only answers to data subjects.

2.2. Activity: adoption of guidance texts

Statistics of the reporting year – adopted texts:

1 new + 4 amended

If applicable: how the total above is divided between data protection, spam and FoI matters

Data protection: 1 new + 2 amended, FoI: 2 amended

Comments:

1 new guidance opinion: Personal Data in Social Protection and Healthcare Sector + 4 amended opinions: codified FoI Guidelines, Public Sector Registers Guidelines, IP-address and Privacy, Disclosure of Students and Alumni Lists

Explanation: the indicator contains all published guidance texts of common character (also referred to as guidelines, opinions, instructions and recommendations etc) which are soft law acts or educational materials and whose distribution is not restricted to the parties of a particular case. The indicator should not contain up-dates of existing texts or publication of (anonymized) case-law decisions.

The indicator covers also guidance papers which are adopted jointly by several DPAs of one (federal) country.

The distinction between soft law acts and educational materials can be complex. However DPAs can use more precise sub-types.

This indicator does not cover guidelines/opinions, which are adopted jointly, by common working groups (such as Article 29 Working Party, Berlin Group etc).

2.3. Activity: approval of self-regulatory acts

Statistics of the reporting year– approved/advised self-regulatory acts:

0

Comments:

Explanation: besides their own guidelines, DPAs advise and/or approve self-regulatory acts of the trade and professional associations. These may be codes of conduct (Art. 27 of the Directive 95/46/EC), as well as certification systems, privacy seal etc.

Approval may be a mandatory procedure or just informal acceptance.

Public sector entities (including private holders of public sector information) may also agree on codes of conduct, transparency seals etc which may cover privacy and transparency aspects at the same time.

The statistical indicator shows the number of all kind of self-regulatory acts with the DPAs involvement – advised or approved.

Binding Corporate Rules are listed not here, but in the section 3.6.1.

Approvals of community-level codes of conduct under Art. 27 (3) of the Directive 95/46/EC are shown in the reports of the Art. 29 Working Party.

2.4. Activity: training sessions and other public events

Statistics of the reporting year – organised/participated training sessions/events:

23

If applicable: how the total above is divided between data protection, spam and FoI matters

Data protection: 13, spam 2, FoI 8

Comments:

Explanation: educational events may be organised by the DPAs themselves or the officials of DPAs may participate as lecturers in an event organised by a third party. It is reasonable to keep all public educational events under the same indicator: lectures, seminars, workshops, conferences etc.

Training sessions organized abroad should also be taken into account.

Training sessions organized for the DPA's own employees should not be taken into account.

Additionally DPAs may use more exact figures (e.g. to divide the indicator between detailed types of events, to show the number of participants etc).

2.5. Activity: media work

Statistics of the reporting year – media events:

Press releases: 14

If applicable: how the total above is divided between data protection, spam and FoI matters

Data protection 10, spam 2, FoI 2

Comments:

Explanation: the indicator covers all media events like press releases, articles, interviews and media shows – if the DPA's representatives were involved.

If DPAs were mentioned in the media without their involvement the events are not taken into account.

Additionally, DPAs may use more exact indicators such as the size of the targeted audience etc.

2.5.1. Sub-activity: work in social media

Statistics of the reporting year – accounts in social media:

1

Comments:

Facebook

Explanation: the indicator covers accounts in social media, edited or co-edited by DPAs. One DPA can have more than one account in the same website for different target groups.

Additionally DPAs may use more exact indicators such as the number of posts, number of followers etc.

2.6. Activity: annual reporting

Powers – we provide a report on our activities:

1 Yes
2 No

If Yes – what is the reporting period:

1 a calendar year
2 or other period:

Comments:

We translate into English only executive summaries

Please add the web-link to the last report

http://www.aki.ee/en/inspectorate/annual-reports in English

Explanation: annual reporting covers many aspects – educational, but also policy advising and disclosure of results of investigation (sometimes contains "name and shame" aspect, too).

There is no need for a special statistical indicator – under normal circumstances there is one ordinary report per reporting period. Possible extraordinary reports are counted under Chapter 4 (Policy advising) as policy opinions.

3. SUPERVISION and ENFORCEMENT ACTIVITIES

3.1. Activity: mediation

Powers - we act or at least we can act as mediator:

1 Yes
2 No

Comments:

Not used, but not forbidden

If applicable: comments on powers in spam or/and FoI matters

Statistics of the reporting year – achieved mediation agreements:

0

If applicable: how the total above is divided between data protection, spam and FoI matters

Explanation: mediation (reconciliation) can be done by request of parties. The procedure may be foreseen by national legislation or used in practice according to customary/unwritten law.

The aim of the proceeding must be the achievement of the reconciliation and agreement between the parties. Also infringement cases (investigations under sub-chapter 3.7) may be finished when the parties make a compromise, but it is not the aim of this type of proceeding.

Specific statistics and comments about amicable resolutions (compromises) done within infringement cases can be shown in the sub-chapter 3.7.3.

3.2. Activity: comparative survey

Powers: we do or at least we can do comparative surveys:

1 Yes
2 No

Comments:

If applicable – comments on powers in spam and FoI matters

The same powers

Specification of powers: we can also make on-the-spot-inspections within the survey:

1 Yes
2 No

Comments:

If applicable: comments on powers in spam and FoI matters

Statistics of the reporting year:

- conducted surveys (all):

9

if applicable: how the total above is divided between data protection, spam and FoI matters

Data protection: 6, FoI: 3

among them: surveys, done in the cross-border cooperation:

1 (GPEN Internet Sweep Day)

- number of all surveyed objects:

148

if applicable: how the total above is divided between data protection, spam and FoI matters

Explanation: comparative survey (or monitoring or "sweep") covers several objects or even a whole sector of economy or public administration. Its main aim is mapping of overall situation, good and bad practices.

Surveys are usually conducted as informal actions without involvement (sometimes even without knowledge) of surveyed organisations. Sometimes surveys are done as extended form of official/formal investigation. Sometimes the DPAs can use both options.

The surveys are usually done by web research or by correspondence. Sometimes the DPAs make on-the-spot-inspections within surveys – if the survey is done as a formal investigation.

DPAs can use results of a survey within its other activities:
a) adopting guidelines,
b) getting input for the trainings and media work,
c) but also taking informal and formal actions in order to ensure compliance.

If a supervisory action covers several organisations, but its nature is formal investigation of infringements and not the mapping of overall situation/good and bad practices, then it has to be described in section 3.7 (as an investigation of infringements).

Some surveys are carried out in coordinated way, by common or similar questionnaire in cross-border cooperation of DPAs. Typical examples of this activity are the annual Internet sweep days, organised by the Global Privacy Enforcement Network (GPEN).

The statistical indicator "number of all surveyed objects" covers only objects surveyed by a DPA itself and not the number of all objects surveyed by all DPAs during cross-border actions.

It depends on a case-by-case basis about how to define the objects of survey – they can be data controllers/processors, but also processing places, information systems (such as databases and mobile applications) etc.

Statistics about all on-the-spot-inspections – including within surveys, audits and authorisations – will be shown together – under activity 3.7.2 (inspections made within infringement investigations).

Informal and formal actions taken on the basis of surveys are statistically shown:

a) as notices according to the sub-chapter 3.3 – if the survey was informal (first of all web-based) action without involvement of surveyed organisations,

b) as results of investigations according to the section 3.7.3 (binding and non-binding decisions or bringing the case before judicial authorities) – if the survey was a formal proceeding.

Otherwise the statistics would be too complicated if they were to show analogical statistical indicators (on-the-spot-inspections, notices, (non)binding decisions etc) repeatedly in different sub-chapters.

3.3. Activity: notice without investigation

Powers: we send or at least we can send notices without investigation:

1 Yes
2 No

Comments:

If applicable– comments on powers in spam and FoI matters

The same powers

Statistics of the reporting year: notices sent without investigations

5

Statistics of the reporting year: number of addressees

34

If applicable: how the total above is divided between data protection, spam and FoI matters

Comments on statistical indicators:

Explanation: In clear and/or minor cases simply a notice without investigation will be sent. The content may be a warning (if there could be a non-compliance) or a recommendation to do something better.

It can be sent:
1) on the basis of complaints, if the DPA does not initiate an investigation itself without a complaint, or
2) without complaints – on the basis of information, obtained from media, from academic researches, from cooperation partners etc or
3) alternatively on the basis of estimative risk parameters alone.

This can be in relation to conducted investigations and audits – if the DPA sends in addition a notice to similar organisations which could be facing similar problems as investigated/audited organisations.

The statistical indicator contains both the number of notices and the number of addressees, while often the number of addressees of the same notice may be significantly larger.

Please bear in mind that this indicator covers only notices sent without investigations.

This indicator does not cover enforcement notices, sent after a binding decision. The enforcement notice informs obligated persons of enforcement actions. It cannot be done without any investigation.

3.4. Activity: preventive audit

Powers: we do or at least we can conduct preventive audits:

1 Yes
2 No

Comments:

a) these audits are mandatory:

1 Yes
2 No

Comments:

b) these audits are consensual:
1 Yes
2 No

Comments:
It is not forbidden to conduct consensual audits, but not used in the practice

c) the final report of the audit is public (even if some parts may be restricted):
1 Yes
2 No

Comments:

If applicable– comments on powers in spam and FoI matters
The same

Statistics of the reporting year: conducted preventive audits (all):
24

If applicable: how the total above is divided between data protection, spam and FoI matters
All in data protection

- among them: audits done as part of cross-border cooperation:
1 (coordinated pan-Baltic audit)

Comments on statistical indicators:

Explanation: preventive audits are concentrating on bigger organisations or organisations processing more sensitive data. Their aim is to help the audited organisation to prevent problems and promote good practices.

If the main aim of the proceeding is to investigate infringements, then it belongs to investigations described under sub-chapter 3-7.

There has to be at least 2 out of 3 characteristics of the preventive audits:
a) they are based on internationally recognised auditing methods,
b) their main aim is to get the bigger/full picture about the audited object, not just to check some narrow particular aspects,
c) they contain on-the-spot-inspections.

These 3 characteristics help us to distinguish preventive audits from usual investigations and from surveys concentrating on some particular narrow aspect or narrowly defined category of data processing.

From a formal point of view, the preventive audits may be:
a) regulated by national legislation as a particular type of procedures,
b) done as an extended form of investigation or
c) done without particular legislative norms.

Sometimes audits are carried out in a coordinated way, by common or similar questionnaire in cross-border cooperation of DPAs. Schengen evaluations are also examples of cross-border auditing.

Statistics about all on-the-spot-inspections – including within audits, surveys and authorisations – will be shown under section 3.7.2 (inspections made within infringement investigations).

Actions taken on the basis of results of audits will be shown under section 3.7.3.(non-binding and binding decisions, bringing cases before judicial authorities).

3.5. Activity: registration

Powers: we keep a public register according to Art. 21 of the Directive 95/46/EC:

1 Yes
2 No

Comments:

Statistics of the reporting year:

- total number of registered data controllers:

1274

If the object of registration is not the data controller, then what the objects are: e.g. data filing systems, security cameras, processing places etc:

Data controllers are registration objects

- total number of registered data protection officers (if the national law provides for their registration):

1588

What the indicator means:

1 the number of controllers who have appointed their DPOs or
2 the number of DPOs despite of the number of controllers they are related to.

- number of all entries made in the register on controllers and DPOs during the reporting period (including changes and deletions):

547

- number of refusals of registration:

0

Explanation: all DPAs have to gather notifications on personal data processing and keep a public register which is containing the notified information. It is regulated by the Art. 18-19 and Art. 21 of the Directive 95/46/EC.

Mostly the objects of registration are data controllers. However it may be regulated differently under national law – e.g. registration objects are data filing systems, not controllers as such.

One exception that can derogate or exempt from the notification obligation, is appointment of a data protection officer (Art. 18 (2) of the Directive 95/46/EC). In some countries data protection officers (DPOs) have to be also notified to and registered with the DPA.

In order to make the statistics comparable it has to be clarified, what the number means – just the number of DPOs (despite the number of controllers they are related to) or the number of data controllers, who have appointed their DPOs.

3.6. Activity: authorisations for personal data processing

Directive 95/46/EC regulates types of authorisation: data transfer to 3rd countries and prior checking.

3.6.1. Sub-activity: authorisation to data transfer to 3rd countries

Powers:

	Yes	No
we can authorise data transfer to 3rd countries:	X	
we do or at least we can do on-the-spot-inspections within authorisation:	X	☐

Comments:

Statistics of the reporting year: authorisations for transfer of personal data to 3rd countries as following:

- transfer authorisations granted on the basis of the EC standard contractual clauses, binding corporate rules and ad hoc contracts.

18

- among them: decisions through mutual recognition given as the leading authority:

0

Explanation: authorisations to transfer of personal data to 3rd countries are done under Art. 25-26 of the Directive 95/46/EC. The indicator categorises the transfers by 3 mechanisms: European Commission's standard contractual clauses, ad hoc contracts and in mutual recognition on the basis of binding corporate rules (BCR).

If a DPA is not able to accept the mutual recognition on the basis of BCR, then instead of BCR the ad hoc contracts indicator is referred to.

Statistics about all on-the-spot-inspections – including within authorisations – will be shown together – under activity 3.7.2 (inspections made within infringement investigations).

3.6.2. Sub-activity: prior checking

Powers: we make or at least we can make prior checks:

1 Yes
2 No

If Yes - who are the objects of prior checking?

If Yes - we can do on-the-spot-inspections within prior checking:

1 Yes
2 No

Statistics of the reporting year: conducted prior checks:

415 (397 controllers of sensitive data protection, 18 approvals to scientific researches without data subjects' consent)

Is the DPAs work done on prior checking also shown under other statistical indicators? If yes, please comment:

The registrations of sensitive data controllers (listed under subchapter 3.5) is formally (but only formally) also prior checking: 303 new controllers, 94 controllers made registration amendments

Explanation: Member States shall, according to the Art. 20 of the Directive 95/46/EC, determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

This is also the difference between audits and prior checking – the latter are done only before certain risky processing as the proceeding granting authorisation.

Some cases may be counted twice in statistics (t.e. as prior checking and in the same time or consequently as registration of data controllers).

Statistics about all on-the-spot-inspections – including within prior-checking – will be shown under section 3.7.2.

Please bear in mind that prior checks for authorisation of personal data processing can be done on the basis of general data protection law and also on the basis of specific acts.

Nevertheless all prior checks done by the DPAs in order to authorise specific processing are prior checks in the meaning of Article 20 of the Directive and have to be counted here.

3.7. Activity: investigation and resolution of infringements

Introduction: the aim of investigation is to terminate the infringement (law violation/offence) and to protect the rights and freedoms (including the access rights) and – but not always – to punish offenders.

Investigation and resolving of infringements (both complaints-based and *ex officio*) are the implementation measures of the:

- Art. 28 (3), (4) of Directive 95/46/EC,

- Art. 15a (1) (2) (3) of the Directive 2002/58/EC,

- Art. 25 (2), (3) of Framework Decision,

- Art. 8 of the Tromsø Convention.

In some jurisdictions the DPAs may initiate proceedings also against adoption of legal acts by parliaments or other public bodies. These cases are also covered by this activity, see the results of these investigations under 3.7.3.c-6: declaring an adopted legal act (or part of it) illegal or unconstitutional.

Investigations may have domestic or international cooperative dimension (engagement or coordination with other regulators or DPAs).

Please pay attention that there may be more than one procedural law for the investigations according to national legislation.

E.g. in many countries the administrative/supervisory law and penal/misdemeanour law are separated. Some powers can be exercised only under administrative law (like coercive fines, substitutive enforcement) and some only under penal law (like compelled attendance at the interrogation).

Power differences/exceptions may also be included depending upon the types of supervised entities (for instance on-the-spot-inspections can be made only in governmental agencies).

Please try to cover all aspects, arisen from all types of the procedural law and from all types of supervised objects. Please try to comment briefly on this kind of power differences/exceptions.

3.7.1. Initiation options

Powers: investigations can be initiated on the basis of:

	Yes	No
a) complaints	X	
b) our own initiative (ex officio)	X	

Comments:

If applicable– comments on powers in spam and FoI matters

The same powers

Statistics:

a) received complaints (even if the investigation will not be formally followed):

390

If applicable: how the total above is divided between data protection, spam and FoI matters

251 in data protection and spam matters, 139 in FoI matters

b) *ex officio* **investigations:**

86

If applicable: how the total above is divided between data protection, spam and FoI matters

83 in data protection and spam matters, 3 in FoI matters (audits included, surveys excluded)

c) notifications on data breaches submitted by data controllers:

5 (telecom sector)

If a complaintive address has been submitted by a person whose own data subjective rights are not infringed and who is not acting as parent, legal guardian or attorney (e.g. addresses submitted by an association acting as defender of public interests), then are the addresses listed under:

1 complaints or

2 ex officio investigations

Explanation: legal rules and thresholds for formal opening of an investigative case are different. Therefore it is reasonable to count all submitted complaints – DPAs have to deal with them anyway, even if the case will formally not open.

Ex officio investigations contain also those investigations based on the notifications of service providers (data controllers) on personal data breaches. Notification obligation is foreseen by Art. 4 (3) of the Directive 2002/58/EC for telecom service providers, but additional obligations may arise from the national law.

However – due to the different national laws – it is important to get the comparable overview how the data breach notification duty works in practice.

3.7.2. Investigative measures

Powers: we can use the following investigative measures:

3.7.2. a) demanding submission of documents, other evidences and explanations (testimonies):

1 Yes
2 No

Comments:

3.7.2. a-1) including requesting data for the identification of the user of the electronic communication devices from telecom service providers:

1 Yes
2 No

Comments:

3.7.2. b) summoning persons to interrogation (into premises of DPA):

1 Yes
2 No

Comments:

3.7.2 c) making inspections on the spot, entering the premises or territory and accessing evidence (like documents, equipment, recorded data):

1 Yes
2 No

Comments:
A search of a private home – on the basis of a permission of a judge

3.7.2. d) requiring persons who are present at the place of inspection to prove their identity during inspections:

1 Yes
2 No

Comments:

3.7.2 e) impose coercive fines (which can be repeated) in order to ensure the investigation (t. e. if a person refuses to give requested information to DPA's investigators).
[Coercive fines imposed after the investigation in order to ensure the enforcement of the resolution should be described under 3.7.3 b-3]

1. Yes
2. No

Comments:
One fine up to 9600 € - it can be repeated endlessly

3.7.2 f) applying substitutive enforcement during the investigation (taking protective or other compliance measures instead of the obligated person; usually the obligated person has to compensate the costs of substitutive enforcement).
[Substitutive enforcement applied after the investigation in order to ensure the enforcement of the resolution should be described under 3.7.3 b-4]

1 Yes
2 No

Comments:

3.7.2 g) other measures not described above:

Public authorities have to react if the DPA asks them to conduct internal supervisory investigation (the superior's supervision).

If applicable– comments on powers in spam and FoI matters

The same powers

Statistics of the reporting year: on-the-spot inspections:

33

If applicable: how the total above is divided between data protection, spam and FoI matters

Data Protection 31, FoI 2

Explanation: the statistical indicator about on-the-spot-inspections covers inspections done during complaints-based and ex officio investigations, surveys, preventive audits and authorisations.

3.7.3. Resolutions

Powers:

3.7.3. a) we can make non-binding decisions:

1 Yes
2 No

Comments:

If applicable – comments on powers make non-binding decisions in spam and FoI matters

The same powers

3.7.3 b) we can make legally binding decisions for:

b-1) imposing obligations (to do something or to stop/avoid doing something):

1 Yes
2 No

Comments:

b-2) imposing financial punishment/penalty (under principle *ne bis in idem* – "not twice in the same thing"):

1 Yes
2 No

Comments:

Cannot used against public authorities, but can used against their employees (not institutional, but personal liability in the public sector).

b-3) imposing coercive fine (which can be repeated):

1 Yes
2 No

Comments:

b-4) applying substitutive enforcement (taking protective or other compliance measures instead of obligated person):

1 Yes
2 No

Comments:

b-5) withdrawing an authorisation:

1 Yes
2 No

Comments:

b-6) taking other measures not previously listed:

Civil service employers have to react if the DPA asks them to open a disciplinary investigation against their civil servants.
The name-and-shame-policy – a black list of spammers published on the DPA's webiste

If applicable – comments on powers to make binding decisions in spam and FoI matters

The same powers

3.7.3 c) we can bring the case before judicial or other competent authority for asking to:

c-1) impose obligations (to do something or to stop/avoid doing something):

1 Yes
2 No

Comments:

c-2) impose financial punishment/penalty (under principle *ne bis in idem* – "not twice in the same thing"):

1 Yes
2 No

Comments:

c-3) impose coercive fine (which can be repeated):

1 Yes
2 No

Comments:

If a state institution/agency ignores the DPA's order, the DPA is entitled to ask a court to impose coercive fine (the judicial coercion)

c-4) apply substitutive enforcement (taking protective or other compliance measures instead of obligated person):

1 Yes
2 No

Comments:

c-5) withdrawing an authorisation:

1 Yes
2 No

Comments:

c-6) declare an adopted legal act (or part of it) illegal or unconstitutional:

1 Yes

2 No

Comments:

The DPA is not entitled to bring cases before the constitutional court (Supreme Court), but the Head of the DPA is entitled to ask the Chancellor of Justice to consider it (the direct reporting rights)

c-7) take other measures not previously listed:

If applicable – comments on powers to bring the case before judicial or other competent authority in spam and FoI matters

The same

Statistics:

a) non-binding decisions:

56

b) legally binding decisions:

59

c) cases brought before judicial or other authorities to make decision:

0

If applicable: what is the proportion of compromise resolutions (amicable resolutions) achieved in infringement cases.

0

If applicable: how the total above is divided between data protection, spam and FoI matters

Non-binding: 46 in data protection and spam matters, 10 in FoI matters.
Binding: 43 in data protection and spam matters(26 concerning the registration/notification duty of sensitive data controllers), 16 in FoI matters

Explanation: the results of the investigation may be:
a) non-binding decisions or
b) binding decisions or
c) bringing the case before judicial or other competent authority.

Non-binding decisions are warnings, recommendations and reprimands on the basis of investigations. Warnings and recommendations sent without investigations are counted under activity 3.3 (notice without investigation).

DPAs may sometimes adopt non-binding decisions even being entitled to make binding decisions.

The decisions are binding, if they are immediately executable/enforceable. It means that an enforcement authority (police, bailiff, huissier de justice etc) is obliged to take enforcement measures by request of the DPA. The enforcement measures can be the use the direct force, expropriation the money from bank accounts, seizure the property and selling it by auctions etc.

If for the taking of enforcement measures is required a new discretionary decision by another authority, it means that the decision of the DPA is just a preliminary, non-binding opinion and not a binding decision.

Complaints submitted to the DPA by mistake and forwarded without its own investigation by the DPA to the right authority are not counted under activity 3.7.3.c.

4. POLICY ADVISING

Powers: we can provide advice to national and/or sub-national policy makers:

1 Yes
2 No

Comments:

We need to be consulted on new legislation proposals:

1 Yes
2 No

Comments:

We need to be consulted when new information systems (databases, registers) are created by public bodies:

1 Yes
2 No

Comments:
Pre-approvals for public sector databases – 139 in year 2016

We are members of permanent bodies advising national or sub-national policy makers:

1 Yes
2 No

Comments if necessary, including names of the advisory bodies
The Council of National Statistics

If applicable: how the advising tasks are applied to spam and FoI matters
The same in FoI matters. Pre-approvals for public sector databases cover also FoI aspects

Statistics of the reporting year:

a) opinions on draft legal acts:
27 (+139 statutes of public sector databases)

b) other policy advices:

If applicable: how it is divided between data protection, spam and FoI matters

Explanation: Policy advising means advising the heads of states, national and regional parliaments, national and regional governments, executive and judicial authorities, local self-governments (municipalities) and other public authorities in policy matters.

Eligible acts for this survey are opinions, extraordinary reports and other recorded policy advice to all public authorities in policy matters.

DPAs can give advice:
a) on own initiative,
b) by request of the public authority or
c) the advisory role may be mandatory in some cases – foreseen by national/regional law.

Mandatory advisory role may also mean a membership in some permanent advisory bodies foreseen by national/regional law. Ad hoc bodies will be not taken into account. Internal working groups and informal bodies, not foreseen by national/regional law, will be not taken into account.

Some DPAs have direct reporting rights to the policy makers (t.e. to the Parliament) – not just for submitting an ordinary annual report, but also extraordinarily in actual matters. Extraordinary reports are

also acts of policy advising. Regular ordinary reporting is the activity 2.6 (annual reporting).

The advisory role of the DPAs is corresponding to the meaning of Art. 28 (2) of the Directive 95/46/EC, but also to the art. 23 of the Framework Decision.

DPAs also carry out the policy advising on the international level – first of all through the Article 29 Working Party which is giving advice to the European Commission. Participation in the international working groups and other fora can be described under Chapter 6.

5. ADDITIONAL ACTIVITIES

Brief description of other activities, powers and main statistics – outside of personal data protection, spam matters and freedom of information:

The pre-approval of and the supervision over public sector databases covers also specific rules (like once-only-submission principle) in addition to data protection and FoI rules.

Explanation: this Chapter covers other activities, carried out by the DPAs, which are not listed in previous chapters.

Some examples of other tasks:
- procedures related to voting systems or to use of the electors' data for political campaigning,
- examining of professional qualifications and certifications (t.e. to information security auditors, data protection officers, freedom of information officers etc). Organising of trainings is covered by activity 2.4 (training and other public events),
- extra functions related to services of digital identity (electronic signing, time sealing),
- extra functions related to enterprises dealing with financial creditworthiness of persons.

This Chapter is reserved only for those activities which are outside of personal data protection, spam matters and freedom of information.

Please avoid adding activities which are already listed in the previous chapters.

Please do not describe here activities, which are not carried out on the basis of general data protection act, but on the basis of specific acts still related to the data protection. Those tasks are still data protection tasks and shall be described under sub-chapter 1.2 (for instance matters related to data protection in the area of public security, national defence and criminal justice) or under Chapter 3 (t.e. specific authorisations under sub-chapter 3.6.2).

Please give the description of additional activities using general terms as much as possible, i.e. without using specific national terminology.

6. INTERNATIONAL GROUPS and FORA

Membership of regular international groups and fora:

- ☒Article 29 Working Party
- ☐Association of Francophone Data Protection Authorities
- ☐Conference of Central and Eastern European Data Protection Commissioners
- ☒Conference of European Data Protection Authorities (“Spring Conference”)
- ☒Consultative Committee of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD)
- ☐Consumer Protection Cooperation Network
- ☒Cooperation between Baltic Data Protection Authorities
- ☐Cooperation between British, Irish and Islands' Data Protection Authorities
- ☐Cooperation between Nordic Data Protection Authorities
- ☒Coordinated supervision over the Eurodac Information System
- ☒Coordinated supervision over the European Internal Market Information System (IMI)
- ☒Coordinated supervision over the European Visa Information System
- ☒Coordinated supervision over the Schengen Information System
- ☐EU Council of Ministers Working Party on Information Exchange and Data Protection (DAPIX)
- ☒Global Privacy Enforcement Network (GPEN)
- ☐Ibero-American Data Protection Network
- ☒International Conference of Data Protection and Privacy Commissioners
- ☒International Conference of Information Commissioners
- ☒International Working Group on Data Protection in Telecommunications (Berlin Group)
- ☒International Working Group on Digital Education
- ☐Joint Supervisory Body of the Eurojust
- ☒Joint Supervisory Body of the European Customs Information System
- ☒Joint Supervisory Body of the Europol Information System
- ☐OECD Working Party on Security and Privacy in the Digital Economy

Other regular groups and fora:

Comments: