EDPS/DPO meeting London - 15 October 2017

Workshop: "Ensure a smooth transition"

Ca 60 minutes: Prepare for the new Regulation *now*
Your Director is committed to data protection and wants to prepare the Agency as much as possible, raise awareness of management and adopt new procedures wherever necessary. He would like to know what concrete steps you recommend him to take for smooth transition to the new Regulation by May 2018.
Your task is **to provide your Director with an "ideal" inventory of actions to be undertaken.**

Methodology:
Please focus on the concrete actions to be undertaken *("what"?*) and the legal basis *("why?").* In the light of the accountability principle (Article 4(2) of Proposal), please structure your action plan/recommendations to the Director as follows:

1) Ensure compliance
- e.g. Establish "record" template, compared to "notifications" add inter alia field on transfers to 3rd countries or int. organisations + information on adequate safeguards in this respect
- Transform notifications to "records" to be kept by Controller (article 31).

2) Demonstrate compliance
- e.g. Update all Privacy statements (article 15 (1)): mention DPO as contact point (article 15 (1)b), include information on transfer to 3rd country+ int. organisations,...

3) Verify compliance
- e.g. Controller to carry out audit or inspection at contractor if necessary, possibly with assistance of DPO (article 29(3)h)). Foresee training on audit/inspections.

If you are not sure where to start: Analyse the Commission's draft proposal. Bear in mind the data subject's perspective and their expectations for *efficient* safeguards. Also recall some of the key changes, inter alia articles 4, 4(2), 26, 27 and 33 of the Commission's draft proposal.

20 minutes: Please reflect individually about how to practically implement the new proposal. Don't think about priorities but write down every concrete action required that comes into your mind (where applicable note also the concrete article in the draft Regulation).
25 minutes: exchange your points with a group of 4-5 other participants to consolidate your findings. Do not start to filter the points, but introduce them to the group and write them down. This is a brainstorming-every idea is welcome! Please write the points down easily readable and put the writers name on top of the sheet (your name helps if we have questions about your sheet).
EDPS colleagues will collect all sheets and complement our draft action plan with your ideas. **The finalized version of the action plan, including your ideas, will be shared on circa next week**.

Feel free to use the result of this common exercise and adapt it to your institution, including establishing priorities. For example you can complement it with columns on "who?" (responsible), "when?", "status" or "actions taken" etc... [1].

[1] Special thanks to the DPOs of the Commission, CEPOL, EIB, ECA, ECHA, EEAS and EIPA's June training participants who inspired our own draft action plan which will be complemented with your ideas.

Exercise

Preliminary ideas combined with DPOs' suggestions

NB: Given that the Commission's proposal for the revision of Regulation (EC) 45/2001 is still under legislative negotiations, the following ideas do not prejudice any formal guidance that the EDPS may and will adopt in the future. Participants are recommended to check regularly the EDPS website. Contributions by participants are highlighted by track changes.

Implement accountability: Ensure - demonstrate –verify

1. Ensure compliance

1.1. Monitoring + regular reporting on progress during transition period to top management (by DPO ?)

1.2. Data protection policies: revise existing policies and implementing rules

1.3. Inventory: update of planned and existing processing operations (eg an excel table) as good practice

1.4. New and existing processing operations: privacy by design and by default (Article 27(1))

1.4.1. Appropriate measures to make sure that privacy is built in as a standard setting of the processing operation (*Privacy by design*)

1.4.2. Only the personal data necessary for each specific purpose of the processing must be processed (*Privacy by default*)

1.4.3. Ensure DPO involvement from the outset – foresee his mandatory consultation in the project vision document template → adapt policies

1.4.4. Establish working group DPO and IT/add DPO to IT steering committee as observer

1.4.5. Take into account EDPS thematic guidelines during design phase

1.5. Record of all processing operations: to be kept by Controller - article 31

- Existing notifications to be archived (set retention period)
- Draft 'record' template
- When transforming existing notifications to records: controllers to update on substance (legal basis, recipients, retention periods, organisational and technical security measures (Articles 27, 27, 33), etc.)
- For processing based on consent: establish template + keep documentation of consent (Article 7). Verify if processing operations are based on children consent (Article 8) + if yes establish templates.
- Record to be kept by Controllers, but DPO could also keep copy

1.6. Data protection risk assessments: to be carried out systematically Article 27(1)

1.6.1. Develop template or customise template (EDPS existing guidelines security measures, upcoming EDPS DPIA paper, including records)

1.6.2. Risk assessment could be an annex to the records

1.7. Data Protection Impact assessment (Article 39) – very limited cases: undertake first screening for which processing operations this new obligation will apply

1.8. Privacy statement: update (also on substance, see above for records), mention DPO as contact point in PS, clear and plain language

1.9. Transfers

1.9.1. require necessity + proportionality assessment of the transfer (Article 9 + recital 16). Maintain trace/record of assessment (article 9(2)), eg cover letter to recipient --> provide template + raise awareness

1.9.2. 3rd countries: Articles 47-52: establish adequate safeguards (article 49)

1.10. Procurement procedures/SLAs/MoUs involving or leading to processing of personal data (Article 29)

1.10.1. Data protection as award criterion + competitive advantage for tenderer (Article 29 (1): Update manuals + future Calls for tender, foresee DPO consultation before launch of procurement procedure

1.10.2. Review contractual clauses templates

- eg no sub-contracting without authorisation by Controller (article 29(2), processor shall maintain record of processing operations (article 32 (2); include processor's duty to notify Controller about security breach "without undue delay" (Article 37(2))

1.10.3. Existing contracts, SLA, MoUs: establish list + ideally amend with new contractual clauses

1.10.4. In case of joint controllership: determine respective roles and responsibilities (article 28)

1.11. Data subjects rights, update procedures/implementing rules for right of access, rectification, data portability etc. (Articles 12-22)

1.11.1. Personal data breach notification procedure (Article 37): establish/revise procedure or include in existing IT incident procedures

1.12. Appoint a DPO as internal counsel and provide him adequate resources (Article 44-47)

1.12.1. DPO should expect and prepare for shift in tasks from ex ante notifications to more monitoring tasks (see also articles 46 (1) b) and (2)).

1.13. Consider budget implications of the above, also in regard to IT applications

1.14. Awareness raising (by DPO and/or EDPS): about changes/novelties of the new proposal

1.14.1. Inform management, to update list of (potential) controllers

1.14.2. Staff (also include it in newcomer information)

1.14.3. Intranet update / presentations

1.15. Revise existing DPO implementing rules

2. Demonstrate compliance

2.1. In general: Document policy, instructions, updated notifications

2.2. Record contacts with data subjects

2.3. Register: good practice that it is kept by DPO + to publish on Internet

2.4. Reply to data subjects‘ requests and follow-up

2.5. Reply to EDPS requests: on records, thematic inquiries, bi-annual monitoring exercises, follow up on data breach notifications, etc

2.6. Data protection trainings on regular basis + inclusion in newcomer training

2.7. Demonstrate that DPO has adequate resources

2.8. Reporting: include data protection in reporting (internal reporting by management and external, eg annual activity report)

3. Verify compliance

3.1. Monitoring transition period by DPO to top management

3.2. Regular compliance checks exercise by the DPO

3.3. Inventory + Register: update regularly to keep it accurate, at least 1-2 times per year

3.4. Follow-up on EDPS recommendations

3.5. Update control Standards: include personal data protection

3.6. Use accountability measuring tool, eg inspired by EDPS questionnaire

3.7. Audits: include personal data protection aspects (explore cooperation DPO/internal auditor)

3.8. Revision of existing procedures during the project lifecycle (eg procurement, leave management etc): take into account possible data protection relevance when underlying processing changes (eg change of legal basis, additional recipients…)

3.8.1. Take into account data protection aspects

3.8.2. Update records

3.8.3. Privacy statement

3.8.4. Concerning data protection by design and by default: review during project/procedure lifecycle in light of state of the art (”at the time of the processing itself”, article 27)