

DATA PROTECTION OFFICERS – LESSONS TO BE LEARNT FROM GERMANY



Dr. Alexander Dix, LL.M.
Catholic University of Porto
2 March 2018

OUTLINE

- Origins of the concept in Germany
- Practical issues
- Lessons to be learnt for GDPR compliance

ORIGINS OF THE CONCEPT

- DPOs were first provided for in Europe in the German Federal Data Protection Act 1977
- Compromise between proponents and opponents of external control in the private sector
- Strict external control (including ex officio-audits) by independent supervisory authorities was established from the start in the public sector, DPOs only introduced later
- DPOs were seen as compensation for weaker external supervision in the private sector (corporate self-monitoring, no ex officio-audits by DPAs until 2001)

PRACTICAL ISSUES IN GERMANY

- Accountability
- Professional qualities
- Conflicts of interest
- Independence
- Resources
- Involvement
- Relations DPO – DPA



ACCOUNTABILITY

- Accountability/responsibility for compliance lies with the **controller**, not the DPO (Art. 5 (2), 24 (1) GDPR). The DPO originally (German Federal DP Act 1977) had to „ensure the implementation of the law“ (without having the necessary powers), later (since 2001) had „to work towards compliance“ by the controller.
- The misconception that the DPO might be held personally liable by data subjects, by the DPA or by the controller deterred many candidates in the past.
- Some controllers thought nominating a DPO was all they had to do to ensure compliance (alibi).
- Data protection is a top priority for management.



PROFESSIONAL QUALITIES

- German law since 1977 has required the „requisite qualification and trustworthiness to fulfill the task“ as necessary professional qualification to become a DPO at a private company (later in a public authority as well).
- This has always posed problems esp. for small and medium sized controllers which lacked qualified staff.
- Solutions: duty of the controller to pay for professional training; rely on internal expertise (legal/technical); appoint external DPOs or jointly with other controllers



CONFLICTS OF INTEREST

Two types of possible conflicts of interest:

- In small and medium-size organisations DPOs are not acting full-time but have other tasks as well. Which tasks are incompatible with DPO function ? **The fox should not be put in charge of the henhouse.**

Incompatible functions are e.g.: chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT department (Art. 29, WP 243)

- More fundamentally an inherent conflict of interest exists where the DPO is an employee of the controller (not an external DPO on the basis of a service contract).



INDEPENDENCE

DPOs in Germany

- are not subject to any directions how to fulfil their task (cf. Art. 38 (3) GDPR);
- must not be penalized for carrying out their functions;
- their designation may only be revoked under restricted circumstances, the DPA may recommend this in case of lack of professional qualification or trustworthiness;
- their contract of employment may only be terminated under the same restricted conditions (even 1 year after the designation has been revoked);
- they report directly to the top management.



RESOURCES

- In Germany controllers have a duty to support their DPOs (see also Art. 38 (2) GDPR).
- In particular they have to provide them with the necessary human resources, working space and financial resources
- However there were until now no sanctions if controllers fail to comply



INVOLVEMENT

- German DPOs have a right to be informed and involved in all issues relating to the protection of personal data (cf. Art. 38 (1) GDPR)
- This has traditionally proved to be a weak spot in reality: controllers (companies as well as public authorities) often bypassed or sidelined their own DPOs when taking important decisions or planning new IT solutions concerning personal data
- This was facilitated by the absence of sanctions



RELATIONS DPO - DPA

- German DPOs may contact and consult with the competent DPA whenever they are in doubt whether the controller is complying with the law. This is the case e.g. when a controller tries to penalize a DPO.
- German DPAs have always understood the DPOs as part of their **professional network** and used several methods of cooperation (e.g. roundtables, jour fixes etc.).
- Some controllers and DPOs misunderstood the DPO's role as „bandog“ to fend off or influence audits by the DPA.
- The DPA under German law has the power to recommend that the designation of a specific DPO be revoked if he/she is incompetent or there is a conflict of interest (in conformity with Art. 58 (6) GDPR).



LESSONS TO BE LEARNT FOR GDPR COMPLIANCE I

- Controllers' and processors' **obligation to designate** DPOs in all public authorities and certain private businesses (Art. 37 GDPR)
- Duty to **avoid conflicts of interest** when choosing the DPO (Art. 38 (6) GDPR)
- **Clear definition and allocation of tasks** (Art. 39 GDPR).
Problem: how „to monitor compliance“ without the necessary powers which lie with the DPA
- **Clear assignment of accountability** to the controller (Arts. 5 (2), 24 GDPR).
- Difference between Arts. 39 GDPR and 33 Dir 2016/680



LESSONS TO BE LEARNT FOR GDPR COMPLIANCE II

- Duty to **support sufficiently and involve timely** the designated DPO
- Duty to facilitate and finance the DPO's continued **professional training**
- Violation of all these duties may be **sanctioned** by imposing administrative fines on the controller of up to 10 000 000 EUR or 2% of the total worldwide annual turnover in case of controllers in the private sector (Art. 83 (4) GDPR; effective sanctions under Art. 57 Dir 2016/680).
- In the public sector this may be excluded by national law (Germany), but in any case the DPA may **order the public authority to comply** with the obligations under the GDPR.






THANK YOU !

I am looking forward
to your questions

dix@eaid-berlin.de

04/03/2018

DR. ALEXANDER DIX



Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection



EAID

14