SQUIRE PATTON BOGGS

GDPR – The Data Protection Officer ("DPO")

Requirement, Role and Implementation

12 January 2017

Your Speakers

Dr. Annette Demmel, Berlin

Rechtsanwältin
Certified Specialist for Information Technology Law
Certified Specialist for Copyright and Media Law

Monika Kuschewsky, Brussels

Rechtsanwältin
Certified Information Privacy Professional/Europe (CIPP/E)
Betrieblicher Datenschutzbeauftragter (GDDcert.)

Overview

SQUIRE PATTON BOGGS

- Background
- Will your company be required to appoint a DPO under the GDPR?
- Role and tasks of a DPO
- Required expertise and skills
- Practical tips
- Conclusion

The General Data Protection Regulation ("GDPR")

SQUIRE PATTON BOGGS

- 4 May 2016: **Publication**
- 25 May 2016: **Date of entry into force**
- As of 25 May 2018: **Date of application**

Including companies that process personal data outside of the EU but offer their goods or services to individuals within the EU

Background

SQUIRE PATTON BOGGS

- EU Data Protection Directive provides for a **voluntary** DPO regime
  - Simplification/exemption from notification in exchange
- The German model
  - Mandatory DPO concept for the private sector since 1977
  - Goals:
    - strengthening effective self-monitoring
    - making state supervision unnecessary as far as possible
- Some EU Member States provide for a voluntary DPO regime, including France, Slovakia and Sweden
- Some EU Member States foresee the appointment of security information officers or security managers, such as Poland and Spain

Mandatory DPO under the GDPR

Article 37

SQUIRE PATTON BOGGS

- DPO requirement applies to both controllers and processors
- No exception for small or medium-sized companies, but risk-based approach
- The GDPR requires the appointment of a DPO in three cases:
  1. Public authorities or bodies (except courts)
  2. Private companies where the "core activities" consist of
     a) processing operations which require "regular and systematic monitoring" of data subjects "on a large scale"
     b) "large scale" processing of sensitive data or data relating to criminal convictions and offences

Mandatory DPO under the GDPR (Continued)

Article 37

SQUIRE PATTON BOGGS

- EU or Member State law may require the designation of DPOs in other situations
- Article 29 Data Protection Working Party ("WP29") encourages the designation of DPOs on a voluntary basis and has issued guidance
  - See "Guidelines on Data Protection Officers ('DPOs')" of 13 December 2016 (and FAQs) http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
- Non-compliance with the DPO obligation constitutes a serious violation, subject to a fine up to €10 million or up to 2% of the total worldwide turnover

Practical tips

- Review WP29 guidance and assess whether or not a DPO must be appointed
  - ✓ Document the internal analysis, including the relevant factors
- Consider a DPO appointment on a voluntary basis
  - ✓ WP29 will apply Articles 37-39 of the GDPR to the DPO

What does “core activities” mean?

SQUIRE PATTON BOGGS

- Key operations to achieve the controller‘s or processor‘s objectives
- Includes all activities where the processing of data forms an inextricable part of the activity
- Excludes support or ancillary functions for the organization‘s main business

- Examples
  - A hospital’s processing of patients’ health records **(+)**
  - An organization’s supporting activities, such as payroll of their own employees or standard IT support **(-)**

What does “large scale” mean?

SQUIRE PATTON BOGGS

- Depends on
  - the number of data subjects concerned
  - the volume of data and/or range of different data items
  - the duration or permanence of the processing
  - the geographical extent

- Examples
  - Processing of customer data in the regular course of business by insurance companies or banks **(+)**
  - Processing of patient data in the regular course of business by a hospital **(+)**
    - But not processing of patient data by an individual physician **(-)**

What does “regular and systematic monitoring” mean?

SQUIRE PATTON BOGGS

- Includes all forms of tracking and profiling on the internet, but is not restricted to the online world
- Regular = ongoing recurring, constantly or periodically
- Systematic = occurring according to a system, organized, methodical or part of a general plan or strategy

- <u>Examples</u>
  - CCTV
  - Behavioral advertising or e-mail retargeting
  - Profiling and scoring for risk assessment (e.g., credit scoring, money laundering detection and fraud prevention)
  - Location tracking
  - Monitoring wellness, fitness and health data via wearable devices

Position of the DPO
Article 38

SQUIRE PATTON BOGGS

- Must be **involved** in all issues relating to data protection
  - Properly and in a timely manner

Practical tips

- Ensure early information and proper consultation of the DPO
- Invite DPO to meetings of senior and middle management and relevant working group meetings
- Develop guidelines or programs that set out when the DPO must be consulted
- Document reasons for not following the DPO's advice

Position of the DPO — Continued

Article 38

SQUIRE PATTON BOGGS

- Necessary resources
  - Active support by senior management
  - Sufficient time, financial resources, infrastructure and staff
  - Access to other services or business units
  - Continuous training

Practical tips

- Inform all staff of DPO's existence and function
- Consider whether it is necessary to set up a DPO team
- Draw up tasks and responsibilities
- Budgeting

Position of the DPO — Continued

Article 38

SQUIRE PATTON BOGGS

- DPO should be in a position to perform his duties and tasks in an independent manner
  - Controller or processor remain responsible for compliance
- DPOs may not be dismissed or penalised for performing their tasks
- DPO must be free from a conflict of interests
  - Cannot hold a position which leads DPO to determine purposes and means of data processing (case by case assessment)
  - Possible conflicting positions (CEO, CFO, CIO, Head of Marketing, Head of HR, but also lower roles)

Practical tips

- Properly draft terms of DPO contract or job description, including secrecy/confidentiality
- Implement safeguards to ensure independence and avoid conflicts of interest

Tasks of the DPO

Article 39

SQUIRE PATTON BOGGS

- Advisory role
  - Vis-à-vis the controller, the processor and their employees
- Monitoring compliance
  - With GDPR and other data protection legislation, but also internal policies
- Advise on data protection impact assessments and monitor performance (upon request)
- Cooperate with supervisory authorities (“SAs”)
- Contact point for SAs and data subjects
  - Contact details of the DPO shall be published and communicated to the SA

Required Expertise and Skills

SQUIRE PATTON BOGGS

- Expert knowledge of data protection law and practices
- Knowledge of business sector and organisation of the controller/processor
- Ability to fulfill the tasks includes personal qualities (integrity) and assertiveness

Practical tips

- ➢ The DPO may be a staff member or an external provider
- ➢ Consider appointing the DPO for the entire group
  - ✓ Must be easily accessible for everyone (contact details, language, resources, availability)
- ➢ In case of a ‘DPO team’, assign a single individual as responsible lead contact

Practical Tips for DPOs

SQUIRE PATTON BOGGS

- Get familiar with the processing activities and existing rules and processes
- Understand the scope of your tasks and responsibilities
  - Statutory tasks versus optional tasks (for instance, maintaining the record of processing activities)
- Identify key issues and contact persons
- Identify budget and other resource requirements
- Draw up a work plan and prioritize
- Regularly attend relevant meetings and speak to employees and senior management (in some countries Works Councils are important)
- Regularly report to senior management
- Keep up to date (training)

SQUIRE PATTON BOGGS

Questions and Answers

Thank you!

SQUIRE PATTON BOGGS

Dr. Annette Demmel

Partner, Berlin
T +49 30 7261 68 108
annette.demmel@squirepb.com

Monika Kuschewsky

Partner, Brussels
T +322 627 11 11
monika.kuschewsky@squirepb.com