

# Dos and Don'ts for DPOs

including on Data Breach Notifications

25 June 2019 ▪ Αθήνα

Christopher Schmidt, CIPP/E CIPM CIPT CBSA

## Fining Practice of German DPAs

3

**100 Fines** (as of June 2019), total amount: **EUR 483,500**; regional differences

### Inadequate T&O Measures

- Storage of passwords of a social network in plain text (password filtering function).

### Unauthorised Disclosure of Health Data

- ... on the Internet due to inadequate internal control procedures.
- ... to the wrong patient by a hospital.

### Other Unauthorised Disclosures

- Account statements to unauthorised 3<sup>rd</sup> parties in online banking.
- Unlawful transfer of data to business successors.
- Visible Email addresses in To: field.

### Unauthorised Data Collection

- ... of all incoming and outgoing calls to a fire department.
- ... through video surveillance and Dashcams.

### Other

- Unlawful promotional emails.

# What should be **done** in any case?

(Hot topics according to the DPAs)

## Data Protection/Privacy Management System

**DOCUMENTATION**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse  
 pharetra risus in sagittis fringilla, nec molestie tortor maximus. Proin ac  
 magna orci. Donec eros neque. In tunc eget mi sit, sodales imperdiet  
 diam. Suspendisse est vel dui a tristique. Suspendisse ac consequat  
 mi, non ullamcorper neque. Integer nec orci lorem. Nunc quam orci  
 porta consetetur sanderisque sed, dacter nec justo. In fribus imperdiet  
 viverra. Sed ornare sed mauris non aliquam. Sed quis augue at mauris  
 interdum volutpat mollis ac tellus. Vivamus non ullamcorper magna.  
 Donec et dolor metus. Ut dui mauris, pellentesque in risus malesuada,  
 feugiat ac cursum sem. Pellentesque porta rutrum est.  
 Feibus ultricies ligula.



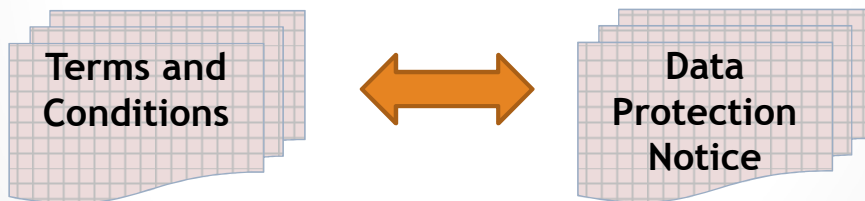
### ORGANISATIONAL STRUCTURE

6

## Data Protection Notice and T&C

Apple Online Store: Higher Regional Court Berlin, judgement of 27 Dec 2018 (case no. 23 U 196/13)

- “Apple Information” and “**Privacy Policy**” (*Datenschutzrichtlinie*), pre-ticked consent boxes
- Terms and Conditions within the meaning of the Unfair Contract Terms Directive 93/13/EEC
- Clauses declared **INEFFECTIVE**. (Data Processing UNLAWFUL!)



7

**Do:** Ensure your independence |

(... and stay alert!)

## Conflict of interests

8

Art. 38(6) GDPR: risk of **SELF-CONTROL** or **EXECUTIVE POSITION** on purposes and/or means of processing, and where economic interests should be considered as a priority

### UNSUITABLE PEOPLE:

- Chief Executive Officer, Chief Operating Officer/ Financial Officer, Marketing/HR Directorate
- IT Manager, System Administrator
- External service providers with dual functions (payroll, file shredding ...)
- Relatives
- Representatives of controllers/processors not established in the EU (Art. 27 GDPR)
- Crosswise Controller/Processor Employees
- AML/Trade Secrets Representative

### POTENTIALLY UNSUITABLE:

- Head or employee of the internal legal department, «Chief Compliance Officer» etc. (+)/(-)
- Quality Management Representative (+)
- Audit staff: reporting obligation to management ⇔ confidentiality (-)
- Lawyers who advise the company on the same subject and who represent it in court (-)
- Members of the Supervisory Board (-)
- Other heads of department (+)/(-)

→ Has an Assistant DPO been appointed?

## Ever thought about

## DPO Liability and

## Potential Insurance Coverage?

- Annual Turnover
- Number of employees in the company
- Sum insured
- Co-payment (“deductible”/“excess”)
- Exclusions? Code of Conduct?
- Contract term, Terms of payment

9

10

## Do: Write a (semi-)annual DPO Report |

*(“Write, and be remembered.”)*

11

## Using metrics to measure your DPMS

KPI (*Key Performance Indicator*): “If you can't measure it, you can't manage/improve it.”

→ Simplification and Illustration, examples:

- 🕒 Number of **confidentiality statements** signed vs. **total number of employees**
- 🕒 No. of employees who have attended data protection **awareness trainings** vs. **total no. of employees**
- 🕒 Ratio of **identified Processors** (Art. 28 GDPR) or **Joint Controllers** (Art. 26 GDPR) to **signed agreements**
- 🕒 Ratio of processing likely to result in a **high risk** to **conducted DPIAs**
- 🕒 Ratio of **complaints received** to total **sanctions imposed** by DPAs
- 🕒 Number of **data breach notifications** to the **DPO**

**Need for Interpretation:**

Successful awareness trainings, or just a lack of information? (employees did not know how to proceed)

12

## Do: Identify joint controllers |

(There could be more than you may think ...)

## Art. 26 GDPR

13

- “two or more controllers jointly determine the *purposes and means of processing*”
- Art. 29 WP, Opinion 1/2010 on the concepts of “controller” and “processor” (WP 169, not endorsed, **to be updated this year**) + Summary of the German Data Protection Conference (German DPAs, “DSK”)
- CJEU: *Wirtschaftsakademie* (C-210/16, “Facebook Fanpages”) + *Jehovah’s Witnesses* (C-25/17)
  - **Joint access** to data not necessary
  - **Joint ≠ Equal**: Different stages/degrees of processing of personal data
  - Definition of **parameters**; accepting pre-determined means of the processing may be sufficient
  - Several DPAs: **no legal basis** for processing (unlike Art. 28 GDPR)
- Further specification in *Fashion ID* (C-40/17), AG’s Opinion: 3rd para. Commercial and advertising purpose, JC’s responsibility limited to those who actively co-decide on the purposes and means of processing

FB Fanpages:  
Investigations of  
German DPAs  
announced

## Art. 26 GDPR—Examples from the German DPAs

14

### Clinical drug trials

- Sponsors, study centres, doctors make decisions on the processing

### Group companies

- Joint management of certain data categories (e.g. address data)

### Joint online platforms

- Several participants pursuing their individual purposes, e.g. Travel reservations processed by a travel agency, hotel chain, and airline

### E-government platform

- Documents available for consultation by citizens; platform operator and the respective authority are jointly responsible (WP169, Ex. No. 11)

### Recruiters/Headhunters

- Screening applicants on behalf of an employer *Abc* and also including applications that were not specifically targeted at jobs at *Abc* (WP169, Ex. No. 6)

### Information pools

- E.g. banks on defaulting customers (WP169, Ex. No. 13)

## Art. 26 GDPR Draft Agreements by the DPA of Baden-Wurttemberg

15

English and Italian translations on my **LinkedIn** profile:

<https://de.linkedin.com/in/christopher-schmidt-law-gdpr>



16

## Do: Understand Breach Notification Timeline |

(Self-reporting or self-denunciation?)

17

8.6.71 Official Journal of the European Communities No L 124/1

REGULATION (EEC, EURATOM) No 1182/71 OF THE COUNCIL  
of 3 June 1971

determining the rules applicable to periods, dates and time limits

*Article 1*

Save as otherwise provided, this Regulation shall apply to acts of the Council or Commission which have been or will be passed pursuant to the Treaty establishing the European Economic Community or the Treaty establishing the European Atomic Energy Community.

*Article 3*

1. Where a period expressed in hours is to be calculated from the moment at which an event occurs or an action takes place, **the hour during which that event occurs or that action takes place shall not be considered as falling within the period in question.**

**5. Any period of two days or more shall include at least two working days.**

2. For the purposes of this Regulation, 'working days' means **all days other than public holidays, Sundays and Saturdays.**



18

## Do: Cooperate with the DPA |

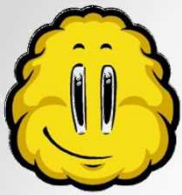
(Be a facilitator, not an obstructor)



# Knuddels

19

- Sep 5, 9:06 pm: An unknown perpetrator published **8,000 member records** on Pastebin (pseudonyms, password, email addresses, first name, place of residence; not all categories in all cases).
- Sep 6, 10:40 am: **Alert email** read by support team and immediately shared within the company.
  - > **Erasure** of the data shared on Pastebin.
  - > **Temporary deactivation** of all known, affected access data.
  - > **Removing unencrypted passwords** in all records.
  - > Developing a module that redirects all members after login to a **password reset** page.
  - > **Checking the servers/logs** for possible attack patterns.
  - > **Notification** of the Knuddels' DPO.
- Sep 7, 1:30 am: Completion of the above measures. Server update. (*Phew!*)



# Knuddels

20

- Sep 7, 2:24 pm: Knuddels receives a link to *nulled.to* → Pastebin with **8,000 further data records**; + link to *mega.nz*, where a data set with **1,872,000 user names** is published.
  - > **Informing** all members asap by email; requiring them to **set a new password** when logging in.
  - > Logins through **unknown devices** will trigger an email/text requesting a password change.
  - > **Encrypting all logfiles** that could possibly contain member data.
- Sep 7, 4:56 pm: Knuddels **informs its users** on the forum, Facebook and Instagram.
- Sep 7, 10:45 pm: Updates rolled out on **German site**. Emails informing users of the data breach and asking them to change their PW on all platforms where they use the same or similar account data.
- Sep 8: **Notification to the competent DPA** of Baden-Wuerttemberg, “*very good cooperation and transparency*”, extensive IT security measures within following weeks, fined **EUR 20,000**
- Root of all evil: **Backup server not updated. Passwords stored unencrypted** (PW filtering function).



22

## Do: Things to keep an eye on |


(Dates, Trends, Tendencies)

23

## Upcoming Important Dates

**EU Commission's Standard Contractual Clauses (SCC, "Standard Data Protection Clauses")**

Schrems II Decision: pending at the Court of Justice of the European Union (CJEU), case no. C-311/18 (*Facebook Ireland and Schrems*).

 Hearing: **9 July 2019**

**European Commission's Privacy Shield Decision (EU) 2016/1250 of 12 July 2016**

*La Quadrature du Net*: European General Court (EGC), case no. T-738/1. (Similar procedure initiated by Digital Rights Ireland, T-670/16, dismissed on grounds of lacking jurisdiction.)

 Hearing: ~~1 and 2 July 2019~~ **Postponed!**

24

## Free Flow Regulation (EU) 2018/1807

EC published pri  
GDPR and the F  
high-frequency

“The Commissi  
contractual cl  
practical imple  
particular impc  
contractual cla  
should be done



EUROPEAN COMMISSION

Brussels, 29.5.2019  
COM(2019) 250 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Guidance on the Regulation on a framework for the **free flow of non-personal data** in the European Union

---

**Contents**

- 1 Introduction
- Purpose of this guidance
- 2 The interaction between the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation - mixed datasets
  - 2.1 The concept of non-personal data in the Free Flow of Non-Personal Data Regulation

sets under the  
data from

ed by model  
ity in the  
l be of  
of the model  
t (which

25

## DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

### of 8 June 2016

### on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

Article 2

#### Definitions

**DE:**  
Geschäft  
schutzge  
(GeschG

**GR:**  
Νόμος 46  
(01.04.20

For the purposes of this Directive, the following definitions apply:

(1) ‘trade secret’ means information which meets all of the following requirements:

- (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- (b) it has commercial value because it is secret;
- (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;**

1 maggio  
63.  
118-670 du  
118  
2018-1126  
/2018

## Professional Associations

26


 New!

### **CEDPO**—Confederation of European DP Organisations:

**German** Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

ARGE Daten, **Austria**

The Association of Data Protection Officers (ADPO), **Ireland**

Association Française des Correspondants à la Protection des Données à Caractère Personnel (AFCDP), **France**

Asociación Profesional Española de Privacidad (APEP), **Spain**

Het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG), **Netherlands**

Stowarzyszenie Administratorów Bezpieczeństwa Informacji (SABI), **Poland**

### **EFDPO**—European Federation of DP Officers:

**German** Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)

Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at, **Austria**

UDPO, Union des DPO, **France**

APDPO Associação dos Profissionais de Proteção e de Segurança de Dados, **Portugal**

Spolek pro ochranu osobních údajů, **Czech Republic**

Spolok na ochranu osobných údajov, **Slovakia**

li Datenschutzverein in Liechtenstein, Liechtenstein

**HADPP - Hellenic Association of dpp, Greece**

27

# Thank you for your attention! |

(Up next: Q&A)