

## PANEL #1

GDPR since May 25, 2018 including enforcement, compliance and the status of the Privacy Shield

**Dr. Nicole Blinn**

**WILMERHALE**

WILMER CUTLER PICKERING HALE AND

# Agenda

- Introduction
- Enforcement and compliance
- Status of the Privacy Shield
- Outlook

WILMERHALE

WILMER CUTLER PICKERING HALE AND

# Introduction

***"We're all going to have to change how we think about data protection."***

That was the message from Elizabeth Denham (UK Information Commissioner at the Information Commissioner's Office), as she delivered a speech on GDPR and accountability on 17 January 2017

# Introduction

contact customer services over the phone, disappointed.

3 1 2

**British Airways** @British\_Airways

Replying to @Jasonhunter1612

To comply with GDPR, please confirm your full name & booking reference. We also need 2 of the following: passport number & expiry date, the last 4 digits of the payment card, billing address & post code, email address. 2/2 ^Kelly

8:38 pm · 16 Jul 18

**Mustafa Al-Bassam** @musalbas

So British Airways is asking for people's personal data over social media "to comply with GDPR", and some people are even replying directly in the public feed.

uwotm8

1:45 AM - Jul 17, 2018

789 572 people are talking about this

1 13 May

i raised several cases so not sure if this is still active as no one has ever responded to any of my cases. I was NOT one of the passengers only delayed for several hours. I was TAKEN OFF THE PLANE.

1 1

**British Airways** @British\_Airways

Replying to [redacted]

Hi Daniel, please delete your previous

27

[redacted] gmail.com >

[redacted] @gmail.com >

[redacted] k@gmail.com >

[redacted] @gmail.com >

[redacted] @googlemail.com >

[redacted] e@gmail.com >

[redacted] @live.co.uk >

[redacted] @outlook.com >

[redacted] @gmail.com >

[redacted] s@gmail.com >

**Chris Kyle** @ChrisPKyle

#GDPR #FAIL @VITLhealth sending out a mass email saying they care about privacy, while visibly copying you in with loads of other people on the same email!!!! #GDPRday #GDPRfail

3:57 PM - May 24, 2018

455 178 people are talking about this

Source: Twitter

# Enforcement and compliance

WILMERHALE

WILMER CUTLER PICKERING HALE AND

# Enforcement and compliance

***“We have got our teeth now, but we haven’t shown our bite”***

(Bundesdatenschutzbeauftragte Andrea Voßkuhl as the head of a German data protection authority put it – *“Wir haben Zähne bekommen, sind aber nicht bissig geworden”*)

***“I expect first GDPR fines for some cases by the end of the year. Not necessarily fines but also decisions to admonish the controllers, to impose a preliminary ban, a temporary ban or to give them an ultimatum,”***

European Data Protection Supervisor Giovanni Buttarelli

# Enforcement and compliance

What enforcement methods does the DPA has to ensure compliance?

- Investigative powers
- Corrective powers
- Impose administrative fines

But don't forget, data subjects have also:

- Right to lodge a complaint with the DPA,
- Right to an effective judicial remedy

# Enforcement and compliance

- Investigative Powers

- DPA has a variety of investigative powers to find out if a violation exists or not.
- DPA may further request access to all personal data and to all information necessary for the performance of its tasks.
- Investigations in the form of data protection audits
- Request information from the processor's or controller's representative
- when necessary the DPA can obtain access to any premises of the controller and the processor, including to any data processing equipment and means.

# Enforcement and compliance

- DPAs have started to audit companies, for example:
  - UK data protection authority investigated companies who provide data analytics for political purposes.  
<https://ico.org.uk/media/fororganisations/documents/2787/guideto data-protection-audits.pdf>
  - May 25, 2017 - a deadline which the Bavarian State Office for Data Protection Supervision (BayLDA) used to send a questionnaire to approx. 150 Bavarian companies on the implementation of the EU-DSGVO. The questionnaire enables companies to determine how far they have already prepared for the new law.

[https://www.la.bayern.de/media/gdpr\\_questionnaire.pdf](https://www.la.bayern.de/media/gdpr_questionnaire.pdf)



















# Enforcement and compliance

Who is next on the list for a data protection audit?

- The BayLDA publishes data protection audits on its website.  
<https://www.lda.bayern.de/en/audits.html>
- These audits can be distinguished by reason, form and scope.
- BayLDA publishes information with regard to on-site examinations of certain controllers. Primarily, the BayLDA wants to advice on selected large scale data protection audits, which they have conducted - online as well as via written submissions - in the past.



# Enforcement and compliance

Privacy audits		
12/2018		
 Deleting Data from ERP Systems (SAP)	Status: Pending	
11/2018		
 Violations of data protection by (sub)processors	Status: Pending	
 Implementation of the GDPR in small and medium-sized enterprises (SMEs)	Status: Running	
10/2018		
 Patch Management eCommerce-Systeme/Online-Shops (Magento)	Status: Running	
 Information duties in application processes	Status: Running	
 Ransomware at medical offices	Status: Running	
 Accountability for large-scale enterprises	Status: Running	
02/2018		
 Patch Management Content Management Systeme (WordPress)	Status: Finished	

# Enforcement and compliance



Violations of data protection by (sub)processors

Status: **Pending**



Start: Open

End: Open

## Brief description

The GDPR has adjusted the notification threshold for so-called "data breaches" to the risk for natural persons resulting from a breach of safety. This led to a significant increase in notifications to the BayLDA pursuant to Art. 33/34 GDPR. What is striking about the notifications so far is that the cause of the risk lies almost exclusively with those responsible in Bavaria. However, since the GDPR also triggers a reporting obligation for those responsible for violations of safety by service providers (even in the case of further subcontracting), the BayLDA wonders why there are hardly any notifications triggered by (international) service providers. The examination should shed light on this question and deals with the "incident response" of larger and data-driven companies.

## Legal basis

Art. 33 GDPR  
Art. 34 GDPR  
Art. 28 GDPR

## Target group

Larger and data-driven enterprises with (presumably) many service providers in an international environment

## Selection criteria

Manual selection of companies where a larger number of (international) contract processing operations can be assumed.


Number of companies audited

15


Number of scheduled on-site audits

7

# Enforcement and compliance

 Accountability for large-scale enterprises

Status: **Running**



Start: 01.10.2018

End: Open

**Brief description**

The GDPR requires the responsible organisation to demonstrate compliance with the GDPR (Art. 5 para. 2 GDPR). This "accountability" represents in principle a "burden of proof reversal", which means that compliance with the legal requirements of the data protection authority must be demonstrated during a control. This means that both the organizational structure of large companies is designed in such a way that other actors (e.g. the legal/compliance department or IT security) deal with data protection requirements in addition to the company data protection officer. In addition, three core processes in the company must be effectively designed in the so-called process organisation:

1. Data protection-compliant processing
2. Dealing with data subjects' rights
3. Dealing with data breaches

Simply put the aim of the audit is to determine compliance with the GDPR in day-to-day business at large companies.

**Legal basis**

Art. 5 para. 2 GDPR  
Art. 24 GDPR

**Target group**

Large-scale and data-driven enterprises

**Selection criteria**

Companies were selected for which the BayLDA assumes that they have already implemented the GDPR in the best possible way. The results of this audit will then define the "benchmark" to be achieved in future audits of other large companies.

**Number of companies audited**

3

**Number of scheduled on-site audits**

3

# Enforcement and compliance

- Selection criteria of data protection audits:
  - Complains of data subjects as an ankle: “7 companies were selected for which there have been frequent privacy complaints at BayLDA lately. The other 8 companies were randomly selected.”
  - Compliance as an ankle: “Companies were selected for which the BayLDA assumes that they have already implemented the GDPR in the best possible way. The results of this audit will then define the "benchmark" to be achieved in future audits of other large companies.”



Questionnaire:

[https://www.lida.bayern.de/media/pruefungen/201810\\_accountability\\_questionnaire.pdf](https://www.lida.bayern.de/media/pruefungen/201810_accountability_questionnaire.pdf)

# Enforcement and compliance

- Corrective Powers of the DPA:
  - Issue **warning** to a controller/processor whose intended processing activities are likely to infringe the GDPR.
  - Issue **reprimands** to a controller/processor whose intended processing activities are likely to infringe the GDPR.

These two instruments constitute the **least severe sanctions** as they do not trigger a direct obligations for the controller/processor to cease or alter their processing activities.

## Enforcement and compliance

- order to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- order to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- order to communicate a personal data breach to the data subject;
- **impose a temporary or definitive limitation including a ban on processing;**
- order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed;
- withdraw a certification;
- **impose an administrative fine pursuant to Article 83;**
- order the suspension of data flows to a recipient in a third country or to an international organization

# Enforcement and compliance

## First formal notice under the GDPR

- The Information Commissioner's Office ("ICO") in the UK has issued the first formal enforcement action under GDPR and the UK Data Protection Act 2018 (the "DPA") Canadian data analytics firm AggregateIQ Data Services Ltd. ("AIQ")
- The enforcement action requires AIQ to "cease processing any personal data of UK or EU citizens obtained from UK political organizations or otherwise for the purpose of data analytics, political campaigning or any other advertising purposes."

Source:

<https://ico.org.uk/action-weve-taken/enforcement/aggregate-iq-data-services-ltd/>

# Enforcement and compliance

- Imposing administrative fines:
  - The most far-reaching powers consist of the imposition of administrative fines.
  - If there is a less serious violation the administrative fines can go up to 10 000 000 EUR (10 million euro), or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
  - In case of more serious violations this goes up to 20 000 000 EUR (20 million euro) or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
  - These fines are substantial and can financially cripple companies.

# Enforcement and compliance

## Has already a DPA imposed fines under the GDPR?

- **Austria** has issued its first fine under the GDPR for an organization that had installed a CCTV camera in front of their establishment but which also recorded images from a large part of the pavement. The DPA issued a moderate fine, **4,800 €**. Large-scale monitoring of public places is not permitted under the GDPR.
- The Barreiro Hospital in Portugal was fined **400,000 €** by the **Portuguese Data Protection Authority CNPD (Comissão Nacional de Proteção de Dados)** for incompliance with the GDPR by not separating access rights to patients' clinical data. The fines were imposed after the Authority had carried out an inspection at the hospital after having been alerted by the medical association.

# Enforcement and compliance

- Data protection authorities seem to be overwhelmed by the GDPR
- The number of:
  - complaints filed by data subjects,
  - requests for guidance, and
  - notifications of personal data breacheshave substantially increased with the data protection authorities.



# Enforcement and compliance

- The data protection authorities need to staff-up, and to prioritize.
- Further, statements from some of the data protection authorities throughout Europe and the general political climate suggest that the authorities will:
  - Focus enforcement activities first on the “big fish”
  - Work with recommendations and warnings before imposing fines against smaller players
  - Continue to issue guidance documents to help companies navigate GDPR
  - But: Take enforcement actions against those that “*persistently ignore their obligations*”

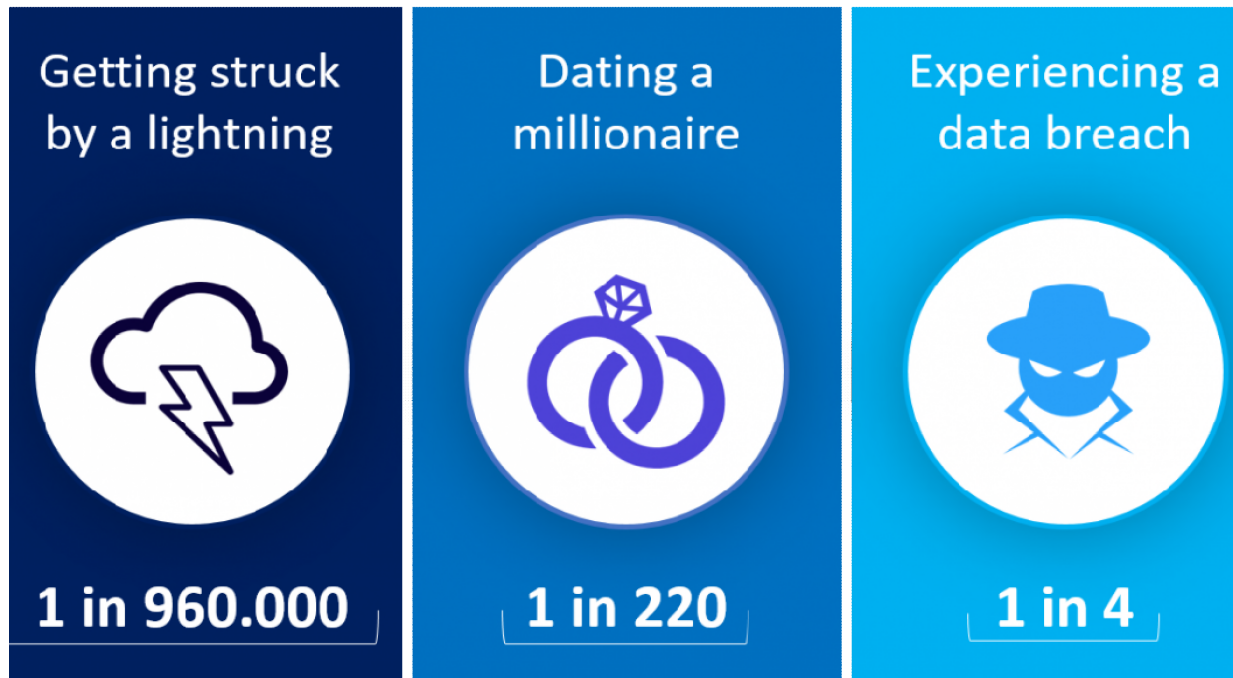
# Enforcement and compliance

## Number of Data Breach Notifications

- In Berlin for example, there were about 130 complaints on 28th May already. Berlin Data Protection Authority has received 1.380 reports in the time from May to July, which is about 10 times higher than in the year before.
- North Rhine Westphalia authority call itself a “call center” because of about more than 100 calls per day in the first month of GDPR.
- France has already seen the volume of complaints increase by more than 50% compared to the year before.
- In the UK the number of reports of data breaches to authorities is four times higher than initially. In June only there have been 1.750 reports, most of them per telephone and about 10% in the health and education sector.
- In Austria 252 data breaches had been notified to the DPA.

# Enforcement and compliance

- Personal Data Breaches happened...



Source: Ponemon Institute's 2017 Cost of Data Breach Study

# Enforcement and compliance

## Data Breach notification

“From 25 May 2018, if you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people’s rights and freedoms, following the breach. When you’ve made this assessment, if it’s likely there will be a risk then you must notify the ICO; if it’s unlikely then you don’t have to report it. **You do not need to report every breach to the ICO.**”

Source: <https://ico.org.uk/for-organisations/report-a-breach/>

# Enforcement and compliance

## The first GDPR court ruling

- Only five days after the GDPR became applicable, the first German court, the Regional Court (*Landgericht*) Bonn (in a decision dated 29 May 2018, case number 10 O 171/18 – in German only), issued a ruling on the practical application of the GDPR
- This probably makes the court's ruling the first GDPR court decision worldwide, and the decision addressed the hot-button issue of public availability of ICANN “WHOIS data”

# Enforcement and compliance

## GDPR as violation of Unfair Competition law?

- Market participants have sent first cease and desist letters to competitors arguing that a violation of GDPR obligations amounts to a violation of the German Act Against Unfair Competition
  - No reported case law on the question whether GDPR violations are actionable by competitors on this basis
  - The German legal commentators and courts appear split on this question
  - There are political initiatives to explicitly exclude GDPR violations from the German Act Against Unfair Competition

## Enforcement and compliance

- By order of September 13, 2018, the Würzburg Regional Court issued an interim injunction against a lawyer who provided an incomplete Privacy Policy on her website as well as an unencrypted contact form. The court further ruled that this also constituted a violation of market conduct rules and accordingly there were injunctive relief claims under the Act against Unfair Commercial Practices. *The court does not mention that the GDPR provisions are final, thus an application of the Act against Unfair Competition relating to data protection violations could be rejected.*
- In a decision dated August 7, 2018, the Regional Court of Bochum rejected a cease and desist claim between competitors due to a violation of the GDPR. In its statement, the Court pointed out that the claimant had no right to obtain a cease and desist decision as the *provisions of the GDPR are exhaustive and therefore exclude claims by competitors*. In its reasoning, the Court expressly referred to a widespread opinion of the legal literature.

# Enforcement and compliance

The GDPR expressly creates a new class action available to data subjects, who will have the right to mandate a not-for-profit body organization or association to act on their behalf: lodge a complaint, take legal action, and receive damage



# Enforcement and compliance

- Austrian privacy campaigner Max Schrems has already launched legal broadsides against internet giants

**Overview of the complaints.** Very similar complaints were filed with four authorities, to enable European coordination. In addition to the four authorities at the residence of the users, the Irish Data Protection Commissioner ([link](#)) will probably get involved in the cases too, as the headquarter of the relevant companies is in Ireland in three cases.

Company	Authority	Maximum Penalty	Complaint
Google (Android)	<a href="#">CNIL</a> (France)	€ 3.7 Mrd	<a href="#">PDF</a>
Instagram	<a href="#">DPA</a> (Belgium)	€ 1.3 Mrd	<a href="#">PDF</a>
WhatsApp	<a href="#">HmbBfDI</a> (Hamburg)	€ 1.3 Mrd	<a href="#">PDF</a>
Facebook	<a href="#">DSB</a> (Austria)	€ 1.3 Mrd	<a href="#">PDF</a>

Source: <https://noyb.eu/>

## Enforcement and compliance

Parliamentary question: “Conmen and cybercriminals have exploited this GDPR-driven paradigm shift by creating new ransomware software to extort money from the vast numbers of companies that are still to comply with the GDPR. Another kind of con consists of playing on the fear of receiving fines by invoicing for bogus compliance operations.

1. Is the Commission aware of these illegal practices?
2. Does it plan to raise awareness among companies and individuals of these con tricks in connection with the GDPR?”

Answer given by Ms. Jourová on behalf of the European Commission:

*[...]“Except where this is allowed pursuant to Article 80 GDPR, other persons wishing to act independently of a data subject’s mandate do not have standing to exercise the rights granted to individuals under the GDPR”[...]*

# Enforcement and compliance



- During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines:  
[https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en)
- <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>
- <https://www.cnil.fr/en/actualite> (PIA-Tool)
- <https://www.la-bayern.de/en/notes.html> (questionnaire and guidelines available)
- <https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo> (DPA templates)

# Status of the Privacy Shield

WILMERHALE

WILMER CUTLER PICKERING HALE AND

# Status of the Privacy Shield

- GDPR, like the EU directive, permits data transfers to countries with adequate protection OR use of approved means:
  - EU Model Clauses
  - Privacy Shield Certification
  - Binding Corporate Rules
  - Derogations
- Being Privacy Shield certified and entering into EU Model Clauses with the data controller are the two most common mechanisms used to transfer personal data from the EU to the US



# Status of the Privacy Shield

## Privacy Shield

Self-certification of US companies to the Department of Commerce

Must be subject to jurisdiction of FTC or DOT who enforces commitments

Privacy Shield Principles: Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse Enforcement and Liability

Requires policy and operational changes

## EU Model Clauses

- Different contractual clauses to be used between EU companies for transfers of data to non-EU companies (data controller to data controller)
- Clauses cannot be revised or changed
- Creates liability giving data subject the direct right of action

## Status of the Privacy Shield

- The future of data transfers under the EU-U.S. Privacy Shield and the EU Model Clauses
  - The Commission approved Privacy Shield last year, but sought additional steps by the United States.
  - The EU parliament adopted a resolution on 5 July 2018 and asked the EU Commission to suspend the EU-U.S. Privacy Shield if the U.S. does not fully comply by September 1st. The European Commission will make a final determination this fall.
  - Second annual review of the Privacy Shield took place in October 2018
  - Currently the Privacy Shield is under legal review regarding the adequate protection of the privacy rights of EU citizens. This “action for annulment” was launched by the Privacy Advocacy Group “Digital Rights Ireland” (case number T-670/16) in hopes of invalidating the Commission’s Adequacy Decision, which approved and adopted the Privacy Shield.

## Status of the Privacy Shield

- On October 19, 2018, European Commissioner for Justice, Consumers and Gender Equality Věra Jourová and U.S. Secretary of Commerce Wilbur Ross issued a joint statement regarding the second annual review of the EU-U.S. Privacy Shield framework.
- The statement highlights the following:
  - a significant number of companies – over 4,000 – have become Privacy Shield-certified since the inception of the framework in 2016;
  - the appointment of three new members to the U.S. Privacy and Civil Oversight Board (“PCLOB”), as well as the PCLOB’s declassification of its report on a presidential directive that extended certain signals intelligence privacy protection to foreign citizens;

# Status of the Privacy Shield

- the regulators' ongoing review of the functioning of the Privacy Shield Ombudsperson Mechanism, and the need for the U.S. to promptly appoint a permanent Under Secretary;
  - recent privacy incidents affecting U.S. and EU residents, with both U.S. and EU regulators reaffirming the “need for strong privacy enforcement to protect our citizens and ensure trust in the digital economy;” and
  - the Commerce Department's promise to revoke the certification of companies that do not comply with the Privacy Shield's principles.
- The European Commission plans to publish a report on the functioning of the Privacy Shield by the end of 2019.

## Status of the Privacy Shield

- Meanwhile, the ECJ has been asked to rule whether Standard Contractual Clauses. This case was brought by Max Schrems, the same plaintiff who triggered the ruling overturning Safe Harbor.



# Outlook

How we prepare for the authority and data subject?

- Have your GDPR documentation ready
- Take data subject requests serious
- Have your data breach response plan in place

# Questions?



## Conctact

Dr. Nicole Blinn, Rechtsanwältin

WilmerHale

Ulmenstraße 37-39

60325 Frankfurt am Main

+49 69 27 10 78 046

[Nicole.Blinn@wilmerhale.com](mailto:Nicole.Blinn@wilmerhale.com)

WILMERHALE

WILMER CUTLER PICKERING HALE AND