

# Recommendations for proceedings before German data protection authorities



## I. Questionnaire in administrative proceedings

## II. Hearings in fine proceedings

## III. Legal proceedings

Administrative questionnaires on data processing, notice of a hearing in administrative fine proceedings or fines already imposed by a data protection authority: In all these cases, your next steps should be carefully considered. If you have been contacted by a data protection supervisory authority, the following tips on how to proceed can provide guidance.

### I. Questionnaire in administrative proceedings

Upon becoming aware of an (alleged) data protection breach, the data protection authority will request the company concerned for a statement as a first step. This often takes the form of an administrative questionnaire. The following should be noted:

#### Step 1: Access to case file

It is advisable to request access to the case file (according to the provisions of administrative law). The case file may contain internal notes drafted by the authority, which are often helpful to understand the background of the administrative proceedings.

#### Step 2: Finding common solution & tactics for statement

It is often recommendable to cooperate and provide information. Otherwise, the authority can take action itself and, for example, carry out on-site inspections at the company premises.

**Caution:** Any submitted statement can be used by the authorities in (additional) fine proceedings. The alleged data protection breach, including all measures taken by the company, must therefore be fully clarified internally before a statement is made.

### Step 3: Termination of proceedings

After clarifying the alleged data protection breach, the authority will often conclude the procedure with a so-called corrective measure. This can take the form of a warning, a reprimand or even a ban of further data processing. It is possible to take legal action against all of these measures.

## II. Hearings in fine proceedings

Data protection violations can be punished with up to 4% of the total annual turnover achieved worldwide. A fine can be issued by the authority in addition (!) to the above-mentioned corrective powers.

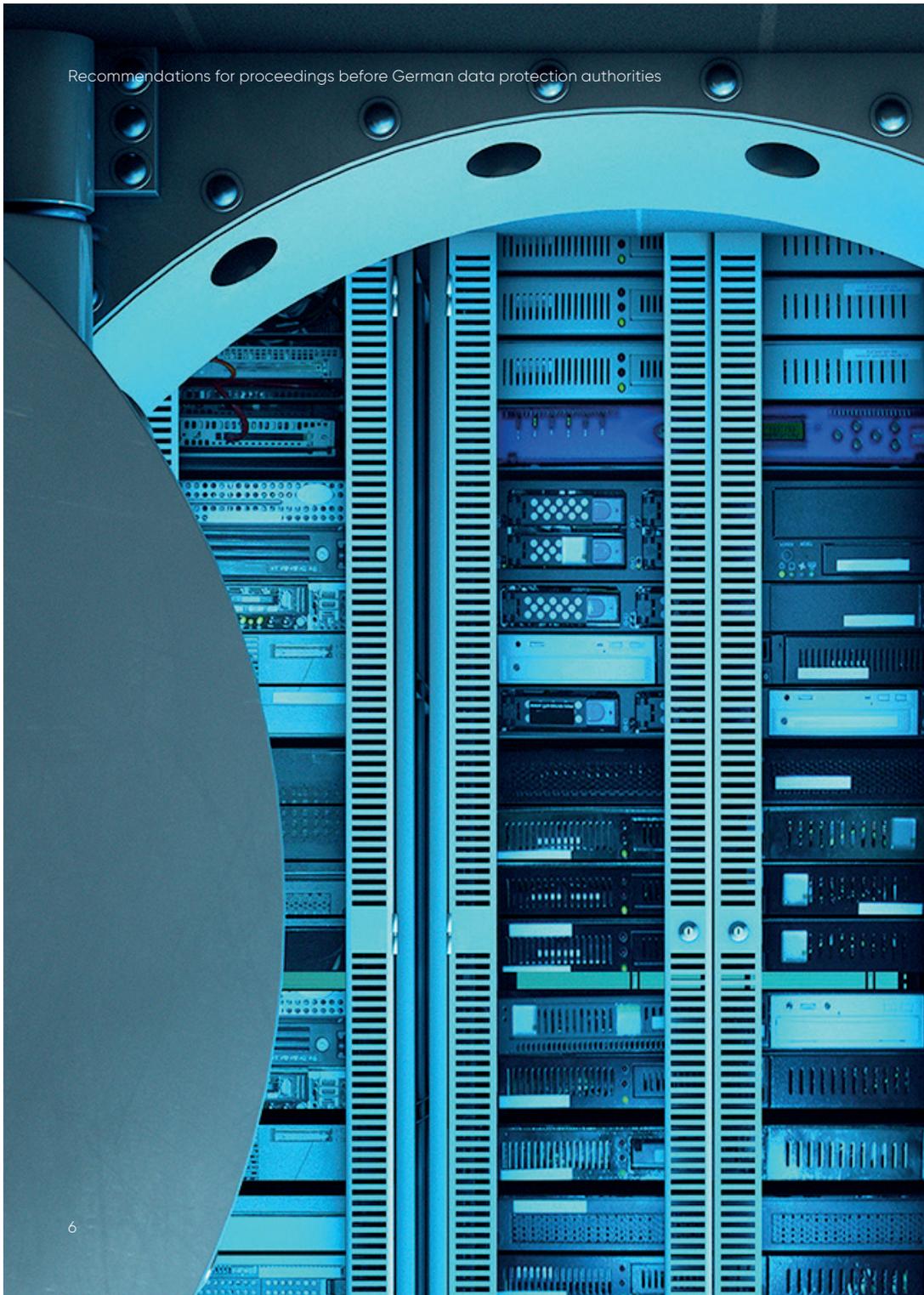
The procedure to impose fines is a formalised process that is governed by the provisions of the law on administrative offences and the Code of Criminal Procedure. For this reason, special procedural principles apply in favour of the company concerned. These include the presumption of innocence and the principle that no one is forced to incriminate himself. The accused must be given the right to be heard before a fining notice is issued. Fining proceedings therefore begin with a notice of hearing from the authorities. The following points are important:

### Step 1: Always request access to case file

Upon receiving a notice of hearing, access to the case file should always be requested (this is governed by the provisions of criminal procedure). The authority is obliged to grant access to the complete investigation file. This also includes complaints by third parties about the alleged data protection breach, on the basis of which the authority started the investigation in the first place.

### Step 2: Defence strategy

The defence strategy depends on the specific alleged offence. Different strategies are possible, ranging from a refusal to provide information on the one hand to a full confession after a previously negotiated maximum fine with the authority (so-called settlement procedure) on the other. You should always consider that the issuance of a fine by an authority can result in negative publicity for the company. This damage to the company's image is difficult to recover once a fine has been imposed for the first time.



### III. Legal proceedings

Legal action is possible both against administrative measures (e.g. a ban on continuing to process data) and against the imposition of fines.

#### 1. Action against fining notices: legal prospects of success vs. media attention

The fines in the H&M case (35.3 million Euros; Hamburg Commissioner for Data Protection and Information Security)<sup>1</sup> and notebooksbilliger.de (10.4 million Euros, Niedersachsen Commissioner for Data Protection)<sup>2</sup> show that the authorities are now outdoing themselves in imposing record fines. However, the fact that such hefty fining notices do not necessarily stand up to judicial scrutiny was recently shown by the ruling of the Regional Court of Bonn in the 1&1 case. Here, the fine of 9.55 million Euros originally imposed by the authorities was reduced by the court to 900,000 Euros<sup>3</sup>. Among other things, the following aspects can be contested in court:

- **Use of information from a reported data breach**  
Findings from duly reported data breaches may not be used by data protection authorities as the (sole) basis for a fining notice.

1 See <https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren> (as at: 10.01.2021).

2 See <https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html> (as at: 10.01.2021).

3 See <https://www.taylorwessing.com/de/insights-and-events/insights/2020/11/lg-bonn-erteilt-bussgeldkonzept-der-deutschen-datenschutzbehoerden-deutliche-absage> (as at: 10.01.2021).

- **Non-compliance with legal requirements**

(here: [German Act on Regulatory Offences, OWiG](#))

The extent to which a data protection breach can be attributed to a company as a legal entity has not yet been clarified by the highest courts in Germany. In some cases, the authorities do not even apply the actually applicable provisions of the OWiG.

- **Amount of the fine not appropriate**

The sole reference to the company group turnover to determine the amount of the fine is not sufficient. Instead, the authority may only use this as one criterion, but must also take into account mitigating circumstances in favour of the company.

Even if the prospects of success in court are promising, the media attention (once again) increased by a court case can be a dissuasive factor. While the press reports extensively on an (alleged) data protection breach, the coverage of a court case that is ultimately won is often minimal. Therefore, any possible judicial success should be carefully considered against the consequences of negative reporting in the decision on how to proceed.

## 2. Overview of instances

### 2.1 Administrative measures and orders

Legal action can be taken against an administrative measure or order. The procedure can be outlined as follows:

#### (a) First Instance: Administrative Court

An administrative measure (e.g. ban on processing certain data) is usually a so-called administrative act. An action against such an administrative act may be brought before the administrative court within one month of its announcement. Preliminary proceedings, in which the legality of the measure is checked again by an authority, do not take place. The court must officially clarify the facts in full. In principle, the decision of the court is made after an oral hearing.

*Time frame: approximately 12 months*

#### (b) Second Instance: Higher Administrative Court

If the administrative court allows an appeal in its first instance judgment (e.g. if the case is of fundamental importance), the appeal may be filed within one month after service of the judgment. The appeal must be substantiated within a further month. The Higher Administrative Court determines whether an oral hearing is required for the decision.

*Time frames: approximately 12 to 24 months*

## 2.2 Fines

When taking legal action against a fine, one should not expect fast results. Fundamental (data protection) legal questions can often only be clarified satisfactorily in the second instance:

### (a) First instance: district or regional courts

In deviation from the usual first-instance jurisdiction of the district courts, the regional courts decide on data protection cases with a fine of 100,000 Euros or more. This special jurisdiction means that the (regional court) judges, who until now have had little practice with data protection and administrative offences law, must familiarise themselves with the new subject matter. Therefore, if fundamental legal questions are involved in the imposition of the fine, one should already plan for the second instance.

*Time frame for interim proceedings and first instance: approximately 6 months to 12 months*

- An objection against the fining notice must first be lodged with the supervisory authority. This objection sets out the legal grounds on the basis of which the fining notice is deemed to be unlawful. On the basis of this objection, the authority is again given the opportunity to review the fining notice itself and, if necessary, to withdraw it (so-called intermediate proceedings). If the authority does not withdraw the fining notice, it forwards the file to the competent court via the public prosecution's office.

- This is followed by the actual court proceedings before the district or regional court. A written statement must be submitted within a time limit set by the court (approximately 4 weeks). In most cases, a decision is made after an oral hearing.

### (b) Second instance: Higher Regional Court

The Higher Regional Courts are competent in the second instance and have special criminal divisions that only deal with fine cases.

*Time frame second instance: approximately 6 to 18 months*

- A complaint of law against the first instance decision must be lodged within one week. This complaint of law must then be substantiated within a further month.
- A decision is made in most cases after an oral hearing.

**Are you looking for legal advice concerning a data protection case?  
Contact our experts:**



**Dr. Axel  
Frhr. von dem Bussche**

Partner, Hamburg  
+49 40 36803-129  
a.bussche@taylorwessing.com



**Dr. Carolin Monsees**

Senior Associate, Hamburg  
+49 40 36803-402  
c.monsees@taylorwessing.com



**Dr. Paul Voigt**

Partner, Berlin  
+49 30 885636-408  
p.voigt@taylorwessing.com

# 1000+ Lawyers

## 300+ Partners

### 28 Offices

#### 16 Jurisdictions

<b>Belgium</b>	Brussels
<b>China</b>	Beijing*   Hong Kong   Shanghai*
<b>Germany</b>	Berlin   Dusseldorf   Frankfurt   Hamburg   Munich
<b>France</b>	Paris
<b>Great Britain</b>	Cambridge   Liverpool   London   London Tech City
<b>Netherlands</b>	Amsterdam   Eindhoven
<b>Austria</b>	Vienna   Klagenfurt*
<b>Poland</b>	Warsaw
<b>Slovakia</b>	Bratislava
<b>South Korea</b>	Seoul**
<b>Czech Republic</b>	Prague   Brno*
<b>Ukraine</b>	Kiev
<b>Hungary</b>	Budapest
<b>USA</b>	Silicon Valley*   New York*
<b>UAE</b>	Dubai

\* Representative \*\* Associated Offices

Europe > Middle East > Asia

[taylorwessing.com](https://www.taylorwessing.com)

© Taylor Wessing 2021

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at [taylorwessing.com/en/legal/regulatory-information](https://www.taylorwessing.com/en/legal/regulatory-information).