10 November 2022

GDPR Sanctions in Practice – Enforcement and Defense

Tim Wybitul
Latham &
Watkins LLP

Dr. Oliver Draf
Volkswagen AG

Privacy+ Security Forum

Speakers

Tim Wybitul

Partner
Latham & Watkins LLP

Dr. Oliver Draf

Chief Privacy Officer
Volkswagen AG

Agenda

Privacy+ Security Forum

1	Current development: More investigations, higher fines
2	Overview: Avoiding GDPR fines
3	Strategic considerations in defending against GDPR fines
4	EDPD Guidelines on the calculation of fines
5	Relevance of fines for damage claims
6	GDPR Damages – Overview and legal framework
7	Excerpt: Referrals to the European Court of Justice
8	GDPR Damages: Defense Strategies

Current development: More investigations, higher fines

Privacy+ Security Forum

Data protection fines – General overview (EU/GER)

Privacy+ Security Forum

€ 746 m	▪ Online-Retailer (CNPD – Luxemburg, 15 July 2021) ▪ Alleged abusive advertising targeting
€ 405 m	▪ Social Media Platform (DPC – Ireland, 2 September 2022) ▪ Data processing of minors: Young people between the ages of 13 and 17 were allegedly able to set up business accounts on the platform. By switching to business accounts, contact information of the juveniles had allegedly been publicly accessible
€ 225 m	▪ Messenger-Service (DPC – Ireland, 2 September 2021) ▪ Alleged breach of transparency obligations
€ 150 m & € 60 m	▪ Internet service provider (CNIL – France, 6 January 2022) ▪ Allegation: no equivalent possibility to reject cookies on websites as easily as to accept them (legal basis: national data protection laws)
€ 60 m & € 40 m	▪ Internet service provider (CNIL – France, 9 December 2020) ▪ Alleged use of tracking cookies for advertising purposes without the consent of the data subjects and lack of data protection notices
€ 35,2 m	▪ Fashion-Company (HmbBfDI – Germany, 1 October 2020) ▪ According to the authority, implementation of disproportionate control measures that affected hundreds of employees of the Nuremberg Service Centre due to their monitoring

More and more GDPR investigations, high fines

Our perception:

More experience

Authorities gain experience in imposing GDPR fines: Increased quality of fine notices, hearing letters and investigation procedures

Cooperation at EU level

Much and close cooperation between authorities at EU level.

The trend goes towards decisions in cooperation or coherence procedures

No established case law

ECJ proceedings take a long time and many relevant issues are not yet before the ECJ or have not yet been subject to a ruling

Turnover-driven catalogue of fines

The EDPB's catalogue for the fine amount is highly turnover-driven. However, this can also be used as a defense

Thinking outside the GDPR box – Example Germany…

Privacy+ Security Forum

In addition to fines under Art. 83 GDPR, also other legal requirements must be observed, e.g.:

- **German Federal Data Protection Act (BDSG):** Criminal liability under section 42 of the BDSG, e.g. also as a connecting factor for section 130 of the Administrative Offences Act (OWiG).
- **German Telecommunications Telemedia Data Protection Act (TTDSG):** Fines under the TTDSG with a maximum fine of EUR 300.000 (Section 28 para. 2 TTDSG)
- **Digital Market Act (DMA) and Digital Services Act (DAS)**: In the future, DMA, DSA etc. will also become relevant
    - Perhaps there will be a court decision in the future on whether insufficient data security can constitute a DMA violation or whether car manufacturers are gatekeepers within the meaning of the DMA
- **National criminal laws:** (Steadily increasing) data protection norms, e.g. in the German Criminal Code (StGB), but also in other national laws - e.g. Section 42 BDSG is often underestimated

GDPR-Fines – Legal framework

“Each supervisory authority shall ensure that the imposition of administrative fines (...) in respect of infringements of this Regulation (...) shall in each individual case be effective, proportionate and dissuasive.”

Different fine ranges

EUR 10 m / 2 % previous year's turnover *resp.*

EUR 20 m / 4 % previous year's turnover

Calculation criteria

e.g. negligence, previous infringements, cooperation with the authority.

Art. 83 para. 2 GDPR

Public authority practice

Increased public communication by the authorities

Guidelines on the calculation of fines

EDPB has published highly turnover-driven guidelines for the calculation of GDPR fines

Overview: Avoiding GDPR fines

Privacy+ Security Forum

Avoiding GDPR fines

Privacy+ Security Forum

Correct implementation of the GDPR helps avoiding (high) fines - but also eases the defense.

Protective measures

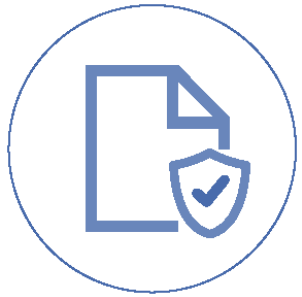
Implement protective measures to avoid data breaches and other incidents

Legal advice

Seek legal advice before introducing new measures and processes

Clear processes

Define clear processes in advance
(e.g. responsibilities in the event of data breaches)



Documentation

Maintain sufficient documentation of all measures in order to be able to demonstrate compliance in the event of proceedings

Example: Data breaches as a trigger for authority procedures

Privacy+ Security Forum

Data breaches attract the attention of the authorities and might be a trigger for authority procedures.

Immediate reaction

Potential obligation to report the data breach to the authorities

Notification of the data breach to data subjects

Calculation of fines

The extent of the cooperation is taken into account in the calculation of the fine (Art. 83 para. 2 lit. f GDPR)

Correct communication with authorities

Privacy+ Security Forum

The GDPR obliges companies to cooperate with authorities – however, companies can also benefit from this.

Early communication

Early communication with authorities and early involvement of advocacy advice is useful

Questioning the authorities

Authorities can also be asked about their legal opinion before measures are implemented.
Attention: This could also bring companies into the focus of the authorities

Consistent communication

Especially in cross-border cases, arguments should be made stringently before various authorities.

Strategic considerations in defending against GDPR fines

Privacy+ Security Forum

Strategic considerations in defending

Privacy+ Security Forum

Is a trial worth it? Considerations on the strategy

Preliminary examination: Is it worth defending?

Risk of "*reformatio in peius*" in the event of judicial review of a GDPR fine

Defence strategy

Which strategy is best?

Conflict defence, plea bargain or sentence defence (or mix)

Cross-border procedures

Additional requirements for cross-border procedures: different timeline and possible higher risks

Press strategy

Preparation of press releases for certain scenarios.
Close coordination of press topics with the responsible authority

Timing of arguments

Weighing up which arguments to put forward and when.
Reason: One should not "help" the authority to issue a better fine notice.

Strategic considerations in defending

Provoke - and denounce - procedural errors!

Functional definition of a company & consequential problems

E.g.: correct instruction of accused party according to Section 136 para. 1 German Code of Criminal Procedure (StPO)?
(Who is "affected party" - the company?)

EDPD Procedure

Check whether the authority was obliged to initiate a cooperation procedure under Art. 60 GDPR before imposing the fine

Complaint of procedural deficits

E.g.: Incomplete inspection of files, possible violation(s) of the right to be heard, too short time limits for submitting statements, insufficient determination of the offence within the meaning of Section 66 OWiG

Observe the statute of limitations

E.g. Dispute regarding the German provision (Section 31 OWiG - 3 years) and effet utile

Strategic considerations in defending

Privacy+ Security Forum

Detect and use substantive errors by the authorities!

Interpretation of the GDPR	Check the procedure of the authority	Disputing the calculation of the fine
• Interpretation problems in case of **unclear wording**; • **No binding effect** of the opinions of authorities on the interpretation of the GDPR for courts; • Reference to technical and legal complexity of processes or allegations	• Has the authority **presented the facts** correctly? • Is the **legal argumentation** of the authority valid? • Is the **time period** of the offence **definite**? • Check the authority's data protection concept: **How does the authority deal with the same problem?** Does it make mistakes itself?	Possibly not taken into account: • **Number** of persons affected • **Willingness to cooperate** of the processing entity • No infringements in the **past** • Intent vs. **negligence**

Strategic considerations in defending

Privacy+ Security Forum

To mitigate the risk of fines and consequential damages, further attention should be paid:

- **Internal communication,** *e.g.* vis-à-vis the board of directors or other management personnel (who may also be specified in more detail in the hearing letter or in the penalty notice)

- **Involvement of relevant corporate functions, *e.g.*:**
  - Risk management
  - Capital market lawyer (examination of possible publication obligations, *e.g.* under the German Securities Trading Act (WpHG))
  - Corporate lawyers (possible liability of executive bodies)
  - Labour lawyers (information duties under industrial constitution law, labour relations)

- **Liability risks** for board members and other decision-makers and functionaries – raise awareness!

EDPD Guidelines on the calculation of fines

Privacy+ Security Forum

EDPD Guidelines on the calculation of fines – Overview

In May 2022, the EDPB has adopted a new model for calculating GDPR fines

Deterrence

Fines should be effective and dissuasive

(Group) turnover

Fines are strongly oriented towards the turnover of the companies

High fines

Fines will increase especially for large companies with a high turnover

(None) Binding validity?

Direct corporate liability

According to the opinion of the EDPB, authorities can also issue fines against the parent company of a group

EDPD Guidelines on the calculation of fines – Weaknesses

Privacy+ Security Forum

Although a certain standardisation of the practice of fines in the EU can be expected - the model also has weaknesses

Turnover as a criterion for assessment?

Decision on the amount of a fine is regulated solely in Art. 83 para. 2 sentence 2 GDPR, but there is no reference to the criterion of turnover

No reduction of the fine for first offences and cooperation

Previous lawful conduct should not be taken into account to reduce fines. Good cooperation with the authorities also does – according to the Guideline – not have a reducing effect

Attribution according to functional concept of enterprise

Liability of the enterprise for acts or omissions of its representatives, without the breach of duty by a manager. (Referral proceedings before the ECJ are also pending (file no. C-807/21))

Non-transparent assessment criteria

It is not comprehensible which violations are to be classified in which severity categories in (low/high/medium)

Relevance of fines for damage claims

Privacy+ Security Forum

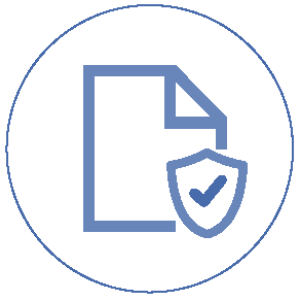
GDPR fines & GDPR damage claims

Privacy+ Security Forum

Civil courts typically adopt the assessments of the data protection supervisory authorities. Successful defence of the fine benefits the successful defence of damages.

No binding effect

Decisions of the data protection supervisory authorities do not have any binding effect on the courts



But: valuations are often adopted

Civil courts increasingly adopt the authorities' assessments, *e.g.* the existence of a GDPR violation

Constantly updated overview of case law in Germany

https://www.lw.com/dsgvo-schadensersatztabelle

GDPR Damages – Overview and legal framework

Privacy+ Security Forum

Case study

- **Press reports about possible data protection violations or data breaches**
  The starting point for (mass) claims for damages under Art. 82 GDPR are often press reports about cybersecurity incidents or possible GDPR violations

- **Example: Data leakage as a breach of Art. 32 GDPR?**
  After a data breach or other data protection violations have become known, plaintiffs' lawyers often argue that the defendant has not ensured sufficient data security and, thus, violated its corresponding obligation under the GDPR

- **Consequences**

- Indications of a data breach or data protection violation become publicly known
- Data protection supervisory authorities start an investigation, possibly with a warning or fine
- Plaintiffs' lawyers, legal service providers and litigation financiers look for such proceedings/indications and place corresponding advertisements etc.
- Customers sue for damages

Litigation financiers

Publicized fine proceedings or data breaches increasingly call commercial litigation financiers or specialized consumer attorneys to the scene

Advertisements

Specific marketing to obtain claimants

GDPR damage claims as a business model

These kind of business models are already established in other areas of law (e.g. compensation claims against airlines)

Examples (Germany)

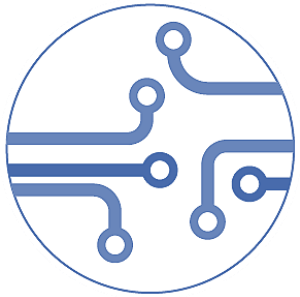
Kleinfee, EuGD, RightNow

Art. 82 GDPR: Liability

“Any person who has suffered material or non-material damage as a result of an infringement […] shall have the right to receive compensation […] for the damage suffered”

Addressee

Art. 82 GDPR addresses the controller or the processor

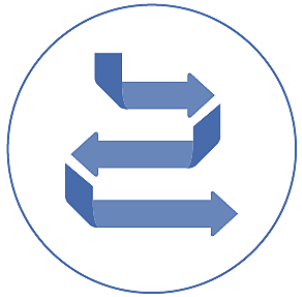


Infringement

Most likely insufficient data security or Art. 15 GDPR violations

Damage

Material or non-material impairments



Causality

The damage must be a result of the infringement

Art. 82 GDPR: Damages

Privacy+ Security Forum

Damages can be of material or non-material nature. The extent of the concept of damages is highly disputed in case law

Extensive approach

A slight impairment can lead to claimable damages

Restrictive approach

The GDPR violation must lead to a concrete, not merely insignificant or perceived violation of personality rights

Risk of abuse

Extension to mere inconvenience?

Excerpt: Referrals to the European Court of Justice

Privacy+ Security Forum

Supreme Court of Austria (15 April 2021)

Privacy+ Security Forum

The Supreme Court asks the ECJ, among other things, if "damage" is a requirement for a claim under Art. 82 GDPR (C-300/21)

1. **Breach equals infringement (?)**
"Does the award of compensation under Article 82 of Regulation (EU) 2016/679 (the GDPR) also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?"

2. **Additional EU law requirements**
"Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?"

3. **Materiality threshold**
"Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence of the infringement of at least some weight that goes beyond the upset caused by that infringement?"

Opinion of the Advocate General (6 October 2022) C-300/21

Privacy+ Security Forum

Advocate General at the ECJ argues against low requirements for non-material GDPR damages

1. **Breach ≠ Damage:** „Therefore, there is an unequivocal requirement that the natural person concerned must have suffered damage as a result of an infringement of the GDPR.“ (para. 28) „[…] Damage continues to be an essential element of civil liability” (Footnote 10)

2. **No punitive damages:** „[…] In EU law, direct awards of so-called ‘punitive damages’ are an exception.”(para. 38) The GDPR makes no reference to the punitive nature of compensation for material or non-material damage; […] From a literal point of view, therefore, it does not allow punitive damages to be awarded” (para. 39)

3. **Loss of control doesn't have to constitute a recoverable damage:** „There is no reason why loss of control over data should necessarily create damage.“ (para. 62) […] lawful processing [...] is also conceivable without the consent of the data subject and thus without [...] exercised control. […]“ (para. 65)

4. **Not all non-material damage is compensable regardless of its seriousness:** „[…] I do not believe, however, that it is possible to infer from this a rule pursuant to which all non-material damage, regardless of how serious it is, is eligible for compensation.“ (para. 105)

5. **Mere anger or annoyance is not compensable damage:** The compensation for non-material damage provided for in the regulation does not cover mere upset which the person concerned may feel as a result of the infringement of provisions of [the GDPR][...] (para. 117)

Opinion of the Advocate General (6 October 2022) C-300/21

Privacy+ Security Forum

The opinion also received criticism. noyb has published a critical analysis of the opinion including – but not limited to – the following:

1. **Damages without damage:** noyb criticizes that the Advocate General is lowering the concept of damage too far. Thus no damages at all would – according to noyb – be possible for GDPR violations in the future

2. **Misunderstanding of „punitive damages“:** The opinion states that non-material damages could lead to punitive damages, which the GDPR does not forsee. noyb argues that this is no argument against non-material damages

3. **Criteria for assessing non-material damages missing:** According to noyb, the Advocate General only gives examples of cases in which **no damages** are awarded. Examples of **when** damages are awarded are missing. Referring to national courts to work out the criteria could lead to inconsistent levels of protection across the EU

4. **Inconsistencies:** noyb points out that from their point of view there are various inconsistencies in the opinion’s reasoning

GDPR Damages: Defense Strategies

Privacy+ Security Forum

GDPR Damages: Defense Strategies

Privacy+ Security Forum

Companies can effectively defend themselves against GDPR damages claims

Preparation

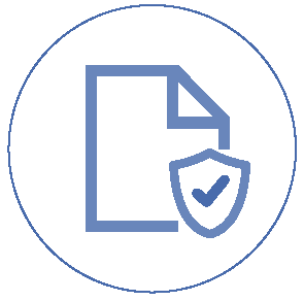
Proper GDPR implementation and implementation of corresponding structures

Defense of fines

Avoiding fine notices that plaintiffs can use to their advantage at trial

Plaintiff's burden of proof?

Reference to plaintiff's burden of proof for GDPR breach, causality and damage



Other arguments

Possible exculpation, reference to materiality threshold [...]

Conclusion

Conclusion

Privacy+ Security Forum

The number of proceedings detrimental to companies is increasing

- Focus of authorities on **large and high-revenue companies**
  - e.g., all triple-digit GDPR fines in the millions were imposed on large U.S. Internet corporations
- The trend is moving away from understandings to **more conflict defense**
- There are more and more proceedings in court due to GDPR fines; from experience, it can be **worth defending oneself against fine notices**
- Courts are lagging behind (in terms of time), many essential questions regarding fines under Art. 83 GDPR are **still unclear**
- There is a lot of work awaiting courts, authorities, companies and lawyers
- The courts will probably look more closely at an excessively strict interpretation of the GDPR by the authorities and at procedural issues

Thank You for Your attention

Privacy+ Security Forum

Questions & Contacts

Tim Wybitul
Partner
Latham & Watkins LLP

Dr. Oliver Draf
Chief Privacy Officer
Volkswagen AG

Disclaimer

Privacy+ Security Forum

This presentation is prepared as a courtesy to Latham clients and friends of the firm. It is not intended to, and shall not, create an attorney-client relationship between any viewer and Latham & Watkins LLP, nor should it be regarded as a substitute for consulting qualified counsel. If you require legal advice concerning this or any other subject matter, do not rely on this presentation, but rather please contact your Latham & Watkins LLP relationship attorney, who can assist you in securing legal advice tailored to your specific situation.

The presentation is not created or designed to address the unique facts or circumstances that may arise in any specific instance, and you should not and are not authorized to rely on this content as a source of legal advice and this seminar material does not create any attorney-client relationship between you and Latham & Watkins.